INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/005482

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, H04L9/32, H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, H04L9/32, H04N7/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-244127 A (Canon Inc.), 29 August, 2003 (29.08.03), Par. Nos. [0098] to [0104]; Figs. 3 to 9 (Family: none)	1-36
Y	JP 2004-72717 A (Hitachi, Ltd.), 04 March, 2004 (04.03.04), Claims 2, 6 to 8; Fig. 3 & EP 1372293 A	1-36
Y	JP 2004-88279 A (Toshiba Corp.), 18 March, 2004 (18.03.04), Figs. 1 to 5 (Family: none)	5,6,8-11, 18-22

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 13 May, 2005 (13.05.05)	Date of mailing of the international search report 31 May, 2005 (31.05.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/005482

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-234728 A (Matsushita Electric Industrial Co., Ltd.), 22 August, 2003 (22.08.03), Claims 73, 74; Fig. 11 & WO 2003/30447 A	13,14,17,24, 25,28
Y	JP 2002-175084 A (Sanyo Electric Co., Ltd.), 21 June, 2002 (21.06.02), Par. No. [0121]; Fig. 10 (Family: none)	13,14,17,24, 25,28

明細書

情報配信システム

技術分野

[0001] 本発明は、情報を配信するためのシステムならびにそれに用いられる端末装置および配信装置に関し、より特定的には、放送を用いて情報を配信するためのシステムならびにそれに用いられる端末装置および配信装置に関する。

背景技術

[0002] 現行のデジタル放送では、受信時に暗号化コンテンツを復号することにより、基本的にコンテンツのリアルタイムな視聴のみを可能としている。そのため、現行のデジタル放送では、放送されるコンテンツを購入し、録画したが後で当該コンテンツを見なかった場合にも、コンテンツの代金を支払わなければならず、必ずしもユーザ利便性が高いサービスとは言えない。そこで、現在、ユーザ利便性の高い新サービスとして、サーバ型放送規格が策定されつつある。

[0003] サーバ型放送では、暗号化コンテンツをそのままハードディスクドライブ等に蓄積し、放送または通信でコンテンツ鍵を取得し、蓄積されている暗号化コンテンツを再生する時に復号化する方式である。これによって、蓄積したコンテンツを後で見なかった場合には、ユーザは、コンテンツを購入しなくてもよくなり、視聴したコンテンツの代金のみを払えばよいため、ユーザ利便性が高いサービスが実現できる。なお、サーバ型放送規格については、ARIB(Association of Radio Industries and Businesses)により発行されているSTD-B25などが詳しい。

[0004] このような多様なサービスが実現可能なサーバ型放送では、ユーザや端末の認証や、各種データの正当性確認のための署名検証などのため、放送経由でPKI(Public Key Infrastructure)に関連する情報(以下、PKI関連情報と記述)を配信することが考えられる。

[0005] 特許文献1には、放送経由でCRL(Certificate Revocation List:証明書失効リスト)などのPKI関連情報を一斉配信することにより、PKI関連情報を効率的に配信するシステムについて記載されている。

特許文献1:特開2002−319934号公報

発明の開示

発明が解決しようとする課題

[0006] しかし、従来のシステムでは、コンテンツの利用とPKI関連情報の取得とが連動していない。したがって、端末に対して、PKI関連情報の受信に対する強制力を働かすことができず、セキュリティを確保できない場合が生じる。たとえば、最新のCRLを受信しなくても、端末側でコンテンツを再生することができてしまうといった事態が生じ、不正サーバや端末を確実に無効化できない。

[0007] それゆえ、本発明の目的は、コンテンツの利用と連動することなく配信されるPKI関連情報を、端末で確実に取得するためのシステムならびにそれに用いられる端末装置および配信装置を提供することである。

課題を解決するための手段

[0008] 上記課題を解決するために、本発明は、以下の特徴を備える。本発明は、コンテンツを配信する配信装置と、配信装置から配信されるコンテンツを受信する端末装置とを備える情報配信システムであって、配信装置は、最新のPKI関連情報の取得を端末装置に要求するためのPKI関連情報取得指示に関する情報を、コンテンツの利用に必要な情報と共に送出し、端末装置は、配信装置から送出されたPKI関連情報取得指示を受信した場合、最新のPKI関連情報を取得することを特徴とする。

[0009] 本発明によれば、コンテンツの利用に必要な情報と共に、PKI関連情報取得指示が送られてくるので、端末装置は、コンテンツの利用と連動して、PKI関連情報を取得することができると共に、取得を強制すべきPKI関連情報を、端末装置に確実に受信させることができる。

[0010] 好ましくは、配信装置は、最新のPKI関連情報の取得を端末装置に要求するためのPKI関連情報取得指示に関する情報を、コンテンツの利用に必要な情報と共に放送するPKI関連情報取得指示放送手段を含み、端末装置は、放送されるPKI関連情報取得指示に関する情報を受信した場合、最新のPKI関連情報を取得するPKI関連情報取得手段を含むとよい。

[0011] これにより、配信装置は、端末装置に対して、コンテンツの利用に必要な情報ととも

にPKI関連情報の取得を指示し、それに応じて、端末装置は、PKI関連情報を取得することとなる。したがって、コンテンツの利用と連動することなく配信されるPKI関連情報を、コンテンツの利用と連動させることができ、その結果、端末側で確実に取得することができる。

[0012] 好ましくは、配信装置は、PKI関連情報取得手段からの要求に応じて、通信網を介して最新のPKI関連情報を端末装置に送信するPKI関連情報送信手段をさらに含み、PKI関連情報取得手段は、配信装置から送信される最新のPKI関連情報を受信するとよい。

[0013] これにより、端末装置は、放送されるPKI関連情報取得指示をトリガとして、通信網を介して最新のPKI関連情報を取得することとなる。

[0014] たとえば、PKI関連情報送信手段は、最新のPKI関連情報をSAC(Secure Authenticated Channel)プロトコルのメッセージに含ませて送信するとよい。

[0015] これにより、安全な通信の下で、PKI関連情報を確実に取得することができ、セキュリティが強化される。

[0016] 好ましくは、PKI関連情報取得指示放送手段は、最新のPKI関連情報を通信で取得するための接続先を、PKI関連情報取得指示に関する情報と共に放送するとよい。

[0017] これにより、端末装置は、指定された接続先に接続することで、PKI関連情報を取得することができる。なお、典型的には、接続先として、配信装置が指定される。

[0018] 好ましくは、配信装置は、当該PKI関連情報を放送信号に多重化して放送するPKI関連情報放送手段をさらに含み、PKI関連情報取得手段は、放送される前記PKI関連情報取得指示に基づいて、放送信号に多重化されて放送される最新のPKI関連情報を取得するとよい。

[0019] これにより、端末装置は、放送されるPKI関連情報取得指示をトリガとして、放送から最新のPKI関連情報を取得することとなる。

[0020] たとえば、PKI関連情報放送手段は、PKI関連情報をMPEG-2 Systems(IEC/ISO13818-1)のプライベートセクションに含ませて放送するとよい。

[0021] たとえば、PKI関連情報放送手段は、PKI関連情報をデータカルーセルに含ませ

て放送するとよい。なお、データカルーセルについては、ARIB STD-B24が詳しい。

[0022] 好ましくは、PKI関連情報取得指示放送手段は、最新のPKI関連情報を放送で取得するための取得先(チャンネルなど)を、PKI関連情報取得指示に関する情報と共に放送するとよい。

[0023] これにより、端末装置は、指定された取得先の放送チャネルからPKI関連情報を取得することができる。なお、一実施形態では、取得先として、エンジニアリングスロット(エンジニアリングトラポン)が指定される。

[0024] 好ましくは、PKI関連情報取得指示放送手段は、限定受信システム(Conditional Access Systems)で用いるECM(Entitlement Control Message:共通情報)またはEMM(Entitlement Management Message:個別情報)にPKI関連情報取得指示に関する情報を含ませて、ECMまたはEMMとコンテンツとを多重化して放送するとよい。なお、ECMやEMMについては、ARIB STD-B25が詳しい。

[0025] これにより、コンテンツの利用のために必須の情報であるライセンス(利用権利、契約情報など)であるECMまたはEMMの受信と同時に、PKI関連情報取得指示を受け取ることができるので、PKI関連情報の更新の強制力が高まる。

[0026] たとえば、PKI関連情報取得指示に関する情報は、PKI関連情報取得指示を示すフラグであり、PKI関連情報取得手段は、フラグを参照して、最新のPKI関連情報を取得すべきか否かを判断するとよい。

[0027] たとえば、PKI関連情報取得指示に関する情報は、PKI関連情報の有効期限、作成日時、バージョン、サイズ、または証明書エントリ数のいずれか、もしくは、これらの組み合わせであり、PKI関連情報取得手段は、端末装置に格納されているPKI関連情報の有効期限、作成日時、バージョン、サイズ、または証明書エントリ数のいずれか、もしくは、これらの組み合わせと、PKI関連情報取得指示に関する情報とを比較することによって、最新のPKI関連情報を取得すべきか否かを判断するとよい。

[0028] 好ましくは、PKI関連情報取得手段は、比較の結果、PKI関連情報が更新されていると判断した場合、最新のPKI関連情報を取得するとよい。

[0029] これにより、PKI関連情報が更新された場合、端末装置は、最新のPKI関連情報を取得することとなる。

[0030] 好ましくは、PKI関連情報取得手段は、配信装置から最新のPKI関連情報をさらに定期的に取得すると良い。

[0031] これにより、PKI関連情報取得指示に応じて配信装置から通信接続でPKI関連情報を取得する場合などにおいて、配信装置の負荷が分散されることとなる。

[0032] たとえば、PKI関連情報は、CRL(Certificate Revocation List:証明書失効リスト)であるとよい。なお、CRLについては、ITU X. 509が詳しい。

[0033] たとえば、PKI関連情報は、公開鍵証明書であるとよい。なお、公開鍵証明書については、ITU X. 509が詳しい。

[0034] 好ましくは、配信装置は、格納するPKI関連情報が更新されたか否かを判断するPKI関連情報更新判断手段をさらに含み、PKI関連情報取得指示放送手段は、PKI関連情報更新判断手段によってPKI関連情報が更新されたと判断された場合、PKI関連情報取得指示に関する情報を、コンテンツの利用に必要な情報と共に放送するとよい。

[0035] これにより、PKI関連情報が更新された場合、端末装置に、PKI関連情報を取得させることができる。

[0036] 好ましくは、PKI関連情報取得手段は、所定の条件を満たすまで、PKI関連情報の取得をリトライするとよい。

[0037] これにより、通信異常などが発生したような場合でも、確実にPKI関連情報を取得することができる。

[0038] 好ましくは、PKI関連情報取得手段によるリトライによっても、PKI関連情報を取得できない場合、コンテンツの利用に関する少なくとも一部の処理が制限されるとよい。

[0039] これにより、PKI関連情報を取得しなければコンテンツの利用が制限されることとなるので、PKI関連情報の取得の強制力が高まる。

[0040] 好ましくは、配信装置は、PKI関連情報を放送信号に多重化して放送するPKI関連情報放送手段と、最新のPKI関連情報の取得を端末装置に要求するためのPKI関連情報取得指示に関する情報を、コンテンツの利用に必要な情報と共に端末装

置に通信で送信するPKI関連情報取得指示送信手段とを含み、端末装置は、配信装置からPKI関連情報取得指示に関する情報が送信されてきた場合、放送されているPKI関連情報を取得するPKI関連情報取得手段を含むとよい。

[0041] これにより、配信装置は、端末装置に対して、PKI関連情報の取得を指示し、それに応じて、端末装置は、放送からPKI関連情報を取得することとなる。したがって、端末装置は、コンテンツの利用に必要な情報とともに送信されてくるPKI関連情報取得指示をトリガとして、放送でコンテンツの利用と連動することなく配信される最新のPKI関連情報を端末側で確実に取得することができる。

[0042] たとえば、PKI関連情報取得指示送信手段は、端末装置へのSACプロトコルのメッセージにPKI関連情報取得指示に関する情報を含ませて送信するとよい。

[0043] たとえば、PKI関連情報取得指示送信手段は、SACプロトコル中で送信するライセンスにPKI関連情報取得指示に関する情報を含ませるとよい。

[0044] たとえば、PKI関連情報放送手段は、PKI関連情報をMPEG−2 Systemsのプライベートセクションに含ませて放送するとよい。

[0045] たとえば、PKI関連情報放送手段は、PKI関連情報をデータカルーセルに含ませて放送するとよい。

[0046] 好ましくは、PKI関連情報取得指示送信手段は、最新のPKI関連情報を放送で取得するための取得先を、PKI関連情報取得指示に関する情報と共に送信するとよい。

[0047] これにより、これにより、端末装置は、指定された取得先からPKI関連情報を取得することができる。なお、一実施形態では、取得先として、エンジニアリングスロットが指定される。

[0048] たとえば、PKI関連情報取得指示に関する情報は、PKI関連情報取得指示を示すフラグであり、PKI関連情報取得手段は、フラグを参照して、最新のPKI関連情報を取得すべきか否かを判断するとよい。

[0049] たとえば、PKI関連情報取得指示に関する情報は、PKI関連情報の有効期限、作成日時、バージョン、サイズ、または証明書エントリ数のいずれか、もしくは、これらの組み合わせであり、PKI関連情報取得手段は、端末装置に格納されているPKI関連

情報の有効期限、作成日時、バージョン、サイズ、または証明書エントリ数のいずれか、もしくは、これらの組み合わせと、PKI関連情報取得指示に関する情報とを比較することによって、最新のPKI関連情報を取得すべきか否かを判断するとよい。

[0050] 好ましくは、PKI関連情報取得手段は、比較の結果、PKI関連情報が更新されていると判断した場合、最新のPKI関連情報を取得するとよい。

[0051] これにより、PKI関連情報が更新された場合、端末装置は、最新のPKI関連情報を取得することとなる。

[0052] 好ましくは、PKI関連情報取得手段は、配信装置から放送される最新のPKI関連情報を、さらに定期的に取得するとよい。

[0053] これにより、PKI関連情報の取得の確度が増すこととなる。

[0054] たとえば、PKI関連情報は、CRLであるとよい。

[0055] たとえば、PKI関連情報は、公開鍵証明書であるとよい。

[0056] 好ましくは、配信装置は、格納するPKI関連情報が更新されたか否かを判断するPKI関連情報更新判断手段をさらに含み、PKI関連情報取得指示送信手段は、PKI関連情報更新判断手段によってPKI関連情報が更新されたと判断された場合、PKI関連情報取得指示に関する情報を、コンテンツの利用に必要な情報と共に端末装置に送信するとよい。

[0057] これにより、PKI関連情報が更新された場合、端末装置に、PKI関連情報を取得させることができる。

[0058] 好ましくは、PKI関連情報取得手段は、所定の条件を満たすまで、PKI関連情報の取得をリトライするとよい。

[0059] これにより、放送異常などが発生したような場合でも、確実にPKI関連情報を取得することができる。

[0060] 好ましくは、PKI関連情報取得手段によるリトライによっても、PKI関連情報を取得できない場合、コンテンツの利用に関する少なくとも一部の処理が制限されるとよい。

[0061] これにより、PKI関連情報を取得しなければコンテンツの利用が制限されることとなるので、PKI関連情報の取得の強制力が高まる。

[0062] また、本発明は、配信装置から配信されるコンテンツを受信する端末装置であって

、コンテンツの利用に必要な情報と共に、配信装置から送出されてくる最新のPKI関連情報の取得を端末装置に要求するためのPKI関連情報取得指示に関する情報を受信した場合、最新のPKI関連情報を取得することを特徴とする。

[0063] 好ましくは、端末装置は、放送信号に多重化して放送される最新のPKI関連情報の取得を要求するためのPKI関連情報取得指示に関する情報を受信するPKI関連情報取得指示受信手段と、PKI関連情報取得指示受信手段がPKI関連情報取得指示に関する情報をコンテンツの利用に必要な情報と共に受信した場合、配信装置から放送されているPKI関連情報を取得するPKI関連情報取得手段とを含むとよい。

[0064] 好ましくは、端末装置は、配信装置から通信で送信されるPKI関連情報取得指示に関する情報を受信するPKI関連情報取得指示受信手段と、PKI関連情報取得指示受信手段がPKI関連情報取得指示に関する情報をコンテンツの利用に必要な情報と共に受信した場合、配信装置から放送されているPKI関連情報を取得するPKI関連情報取得手段とを含むとよい。

[0065] 好ましくは、放送される最新のPKI関連情報の取得を要求するためのPKI関連情報取得指示に関する情報を受信するPKI関連情報取得指示受信手段と、PKI関連情報取得指示受信手段がPKI関連情報取得指示に関する情報を受信した場合、配信装置から最新のPKI関連情報を通信で取得するPKI関連情報取得手段とを含むとよい。

[0066] また、本発明は、コンテンツを端末装置に配信する配信装置であって、最新のPKI関連情報の取得を端末装置に要求するためのPKI関連情報取得指示に関する情報を、コンテンツの利用に必要な情報と共に送出することを特徴とする。

[0067] 好ましくは、PKI関連情報を放送信号に多重化して放送するPKI関連情報放送手段と、最新のPKI関連情報の取得を端末装置に要求するためのPKI関連情報取得指示に関する情報を、コンテンツの利用に必要な情報と共に放送するPKI関連情報取得指示放送手段とを含むとよい。

[0068] 好ましくは、PKI関連情報を放送信号に多重化して放送するPKI関連情報放送手段と、最新のPKI関連情報の取得を端末装置に要求するためのPKI関連情報取得

指示に関する情報を、コンテンツの利用に必要な情報と共に端末装置に通信で送信するPKI関連情報取得指示送信手段とを含むとよい。

[0069] 好ましくは、最新のPKI関連情報の取得を端末装置に要求するためのPKI関連情報取得指示に関する情報を放送するPKI関連情報取得指示放送手段を含み、端末装置に通信で最新のPKI関連情報を取得させるとよい。

発明の効果

[0070] 本発明によれば、配信装置内でPKI関連情報が更新された場合、必ず、端末装置は、最新のPKI関連情報を取得することとなるので、コンテンツの利用と連動することなく配信されるPKI関連情報を端末装置で確実に取得するためのシステムが提供されることとなる。これにより、セキュリティ確保と、PKI関連情報を配信するコストの低減とが図られることとなる。特に、PKI関連情報の取得を指示するための情報を、コンテンツ利用に必須となるECMやEMM、ライセンスなどに含めるようにしているので、最新のPKI関連情報の取得を確実なものとすることができる。

[0071] 本発明のこれらおよび他の目的、特徴、局面、効果は、添付図面と照合して、以下の詳細な説明から一層明らかになるであろう。

図面の簡単な説明

[0072] [図1]図1は、本発明の第1の実施形態に係る情報配信システムの機能的構成を示すブロック図である。

[図2]図2は、配信装置100のECM生成部102が生成するECMのデータ構造を示す図である。

[図3]図3は、第1の実施形態に係る情報配信システムにおける配信装置100および端末装置200の動作を示すフローチャートである。

[図4]図4は、本発明の第2の実施形態に係る情報配信システムの機能的構成を示すブロック図である。

[図5]図5は、配信装置110のECM生成部102が生成するECMのデータ構造を示す図である。

[図6]図6は、第2の実施形態に係る情報配信システムにおける配信装置110および端末装置210の動作を示すフローチャートである。

[図7]図7は、本発明の第3の実施形態に係る情報配信システムの機能的構成を示すブロック図である。

[図8]図8は、配信装置120から送信される通信メッセージのデータ構造を示す図である。

[図9]図9は、第3の実施形態に係る情報配信システムにおける配信装置120および端末装置220の動作を示すフローチャートである。

符号の説明

[0073] 100, 110, 120 配信装置

200, 210, 220 端末装置

101 ECM情報蓄積部

102 ECM生成部

103, 113, 122 放送信号多重送信部

104 PKI関連情報取得指示付加判定部

105 PKI関連情報蓄積部

106, 124 情報取得要求処理部

107 第1の通信部

111, 121 PKI関連情報読出部

123 情報取得指示付加判定部

125 ライセンス蓄積部

201 チャンネル選択部

202, 212, 221 放送信号受信分離部

203, 211, 222 PKI関連情報選択受信部

204 ECM取得部

205, 224 PKI関連情報取得判定要求部

206 PKI関連情報保持部

207 第2の通信部

208, 223 PKI関連情報更新部

225 ライセンス情報取得部

226 ライセンス要求部

発明を実施するための最良の形態

[0074] (第1の実施形態)

図1は、本発明の第1の実施形態に係る情報配信システムの機能的構成を示すブロック図である。図1において、情報配信システムは、配信装置100と、端末装置200とを備える。なお、図1において、端末装置200は、一つであるとしたが、二つ以上であってもよい。この場合、各端末装置は、配信装置100からの放送を受信し、かつ配信装置100と通信網を介して通信可能であればよい。

[0075] 配信装置100は、ECM情報蓄積部101と、ECM生成部102と、放送信号多重送信部103と、PKI関連情報取得指示付加判定部104と、PKI関連情報蓄積部105と、情報取得要求処理部106と、第1の通信部107とを含む。

[0076] ECM情報蓄積部101は、ECM(Entitlement Control Message:共通情報)の生成に必要な情報(以下、ECM情報という)を格納する。

[0077] PKI関連情報蓄積部105は、CRL等のPKI関連情報を格納する。

[0078] PKI関連情報取得指示付加判定部104は、CRLの更新がなされているか否かを判断して、PKI関連情報を取得するための指示に関する情報(以下、PKI関連情報取得指示という)をECMに付加するか否かを判断する。

[0079] ECM生成部102は、ECM情報蓄積部101に格納されているECM情報を取得して、必要に応じて、当該ECM情報にPKI関連情報取得指示を付加して、送信すべきECMを生成し、放送信号多重送信部103に渡す。

[0080] 放送信号多重送信部103は、MPEG−2などのコンテンツの放送信号とECMとをMPEG−2トランスポートストリーム(TS)で多重化して、放送する。

[0081] 第1の通信部107は、端末装置200とインターネット等を介して接続されている。第1の通信部107は、端末装置200から送られてくるPKI関連情報取得要求を情報取得要求処理部106に渡す。

[0082] 情報取得要求処理部106は、端末装置200からPKI関連情報取得要求がなされた場合、PKI関連情報蓄積部105から必要なPKI関連情報を取得して、第1の通信部107を介して、端末装置200に返信する。

[0083] 端末装置200は、チャンネル選択部201と、放送信号受信分離部202と、PKI関連情報選択受信部203と、ECM取得部204と、PKI関連情報取得判定要求部205と、PKI関連情報保持部206と、第2の通信部207と、PKI関連情報更新部208とを含む。

[0084] PKI関連情報保持部206は、配信装置100から取得したCRLや公開鍵証明書などのPKI関連情報を格納し、ライセンスを配信するサーバやホームネットワーク上の他の端末の認証時などに用いたりする。

[0085] チャンネル選択部201は、再生すべきコンテンツのチャンネルを選択する。

[0086] 放送信号受信分離部202は、チャンネル選択部201によって選択されたTSからコンテンツTSと、ECMのTSと、プライベートセクションとして多重されているPKI関連情報のTSなどとを分離する。放送信号受信分離部202は、分離したECMやPKI関連情報のTSを、PKI関連情報選択受信部203およびECM取得部204に渡す。なお、コンテンツのTSについては、図1に図示しないコンテンツ取得部に渡す。

[0087] PKI関連情報選択受信部203は、ユーザからの指示に応じて、放送信号からPKI関連情報のTSを取得し、PKI関連情報を再構成して、PKI関連情報更新部208に渡す。PKI関連情報選択受信部203は、配信装置100からのPKI関連情報取得指示が無い場合であっても、適宜PKI関連情報を取得する。但し、放送異常などの事態や、悪意あるユーザによるPKI関連情報の取得妨害などの事態により、PKI関連情報の確実な取得ができない場合が有り得るものである。

[0088] ECM取得部204は、放送信号受信分離部202によって分離されたECMを取得し、PKI関連情報取得判定要求部205に渡す。なお、ここでは、ECM自体をPKI関連情報取得判定要求部205に渡すようにしたが、ECMにPKI関連情報取得指示が含まれている場合のみ、ECMからPKI関連情報取得指示をPKI関連情報取得判定要求部205に渡すようにしても良い。

[0089] PKI関連情報取得判定要求部205は、ECMにPKI関連情報取得指示が含まれている場合、PKI関連情報保持部206に格納されているPKI関連情報を参照して、PKI関連情報を取得すべきか否かを判断し、取得すべきであると判断した場合、第2の通信部207に対して、PKI関連情報取得要求を配信装置100へ送信させる。

[0090] 第2の通信部207は、PKI関連情報取得要求に応じて配信装置100から送信されてくるPKI関連情報を受信して、PKI関連情報更新部208に渡す。また、配信装置100との通信では、安全な通信を行うため、SACを確立してから通信を行う。

[0091] PKI関連情報更新部208は、PKI関連情報選択受信部203または第2の通信部207から渡されるPKI関連情報をPKI関連情報保持部206に格納して、PKI関連情報を更新する。

[0092] 図2は、配信装置100のECM生成部102が生成するECMのデータ構造を示す図である。図2において、ECMは、ECMセクションの中に、セクションヘッダ、ECM本体、および誤り検出情報(セクションテーラ)を含む。ECM本体は、コンテンツ鍵(あるいはスクランブル鍵)、最新CRLバージョン番号、可変長のプライベートデータ、および改ざん検出情報からなる。ここで、最新CRLバージョン番号は、最新のCRLのバージョン番号を示す。最新CRLバージョン番号が、ECM生成部102で付加されるPKI関連情報取得指示である。

[0093] 図3は、第1の実施形態に係る情報配信システムにおける配信装置100および端末装置200の動作を示すフローチャートである。以下、図3を参照しながら、第1の実施形態に係る情報配信システムにおける配信装置100および端末装置200の動作について説明する。

[0094] まず、配信装置100のPKI関連情報取得指示付加判定部104は、PKI関連情報蓄積部105に格納されているCRLが更新されているか否かを判断する(ステップS101)。なお、PKI関連情報取得指示付加判定部104は、最後にPKI関連情報取得指示を付与した日時(以下、PKI関連情報取得指示付与日時と記す)を保持し、PKI関連情報蓄積部105は、現在(最新)のバージョンのCRLの更新日時も保持していることとする。したがって、PKI関連情報取得指示付加判定部104は、内部で保持しているPKI関連情報取得指示付与日時と、現在のバージョンのCRLの更新日時とを比較することによって、CRLが更新されたか否か、つまり、端末装置200に最新CRLの取得を指示すべきか否かを判断することができる。あるいは、CRLの更新日時が保持していない場合であっても、バージョン番号を昇順または降順でCRLに付与するように運用すれば、CRLが更新されたか否かを判定することができる。

[0095] なお、上記ではCRLの更新日時を用いることにより、CRLが更新されているか否かを判定するようにしたが、PKI関連情報取得指示付加判定部104で、最後に送出したCRLのバージョン番号を記憶しておき、PKI関連情報蓄積部105の最新のCRLのバージョン番号と比較することにより、CRLの更新判定を行うようにしても良い。この場合、ステップS101に先立ち、ステップS102を実行することとなる。

[0096] CRLが更新されていないと判断された場合、つまり、PKI関連情報取得指示付与日時が最新バージョンのCRLの更新日時より新しい場合、ECM生成部102は、PKI関連情報の取得を指示する必要がないと判断し、PKI関連情報取得指示が付加されていないECMを生成して、ステップS104の動作に進む。なお、PKI関連情報取得指示付与日時が最新バージョンのCRLの更新日時より新しい場合であっても、一定期間はPKI関連情報取得指示を行うようにすることも可能である。

[0097] 一方、CRLが更新されていると判断された場合、つまり、PKI関連情報取得指示付与日時が最新バージョンのCRLの更新日時より古い場合、PKI関連情報取得指示付加判定部104は、PKI関連情報の取得を指示する必要があると判断し、最新のCRLのバージョン番号をPKI関連情報蓄積部105に格納されているCRLから読み出して、ECM生成部102に渡す(ステップS102)。次に、ECM生成部102は、ECM情報蓄積部101に格納されているECM情報を読み出し、ステップS102で取得したCRLのバージョン番号をPKI関連情報取得指示として読み出したECM情報に付加して、ECMを生成し(ステップS103)、ステップS104の動作に進む。なお、ECMはコンテンツ毎に送出される情報であるが、ユーザが全てのコンテンツを視聴するわけではないので、コンテンツ毎にPKI関連情報取得指示の付与を区別するようにしても良い。

[0098] ステップS104において、放送信号多重送信部103は、生成されたECMをコンテンツに多重して、放送する。

[0099] 端末装置200の放送信号受信分離部202は、受信信号をチャネル選択して、ECMをECM取得部204に渡す(ステップS201)。

[0100] 次に、PKI関連情報取得判定要求部205は、ECM取得部204が取得したECMに最新CRLバージョン番号が含まれているか否かを判断して、PKI関連情報取得指

示がなされているか否かを判断する(ステップS202)。

[0101] PKI関連情報取得指示がなされていない場合、端末装置200は、PKI関連情報取得に関する処理を終了する。それと並行して、端末装置200は、コンテンツ利用部(図示せず)において、コンテンツを再生する。

[0102] 一方、PKI関連情報取得指示がなされている場合、PKI関連情報取得判定要求部205は、PKI関連情報保持部206が格納しているCRLのバージョン番号を取得する(ステップS203)。

[0103] 次に、PKI関連情報取得判定要求部205は、ECMに含まれていた最新CRLバージョン番号と、PKI関連情報保持部206が保持しているCRLのバージョン番号とを比較して、保持しているCRLが最新のものであるか否かを判断する(ステップS204)。

[0104] 保持しているCRLが最新のCRLである場合、端末装置200は、処理を終了する。それと並行して、端末装置200は、コンテンツ利用部(図示せず)において、コンテンツを再生する。

[0105] 一方、保持しているCRLが最新のCRLでない場合、次にPKI関連情報取得判定要求部205は、最新のCRLを送信させるためのPKI関連情報取得要求を第2の通信部207に送信させる(ステップS205)。

[0106] これに応じて、配信装置100は、PKI関連情報取得要求を受信する(ステップS105)。次に、情報取得要求処理部106は、最新のCRLをPKI関連情報蓄積部105から取得し、第1の通信部107に当該CRLを端末装置200宛に送信させる(ステップS106)。

[0107] これに応じて、端末装置200の第2の通信部207は、最新のCRLを受信して、PKI関連情報更新部208に渡す(ステップS206)。次に、PKI関連情報更新部208は、PKI関連情報保持部206に格納されているCRLを最新のCRLに更新して(ステップS207)、処理を終了する。それと並行して、端末装置200は、コンテンツ利用部(図示せず)において、コンテンツを再生する。

[0108] このように、第1の実施形態によれば、配信装置内でのCRLが更新された場合、PKI関連情報取得指示を含んだECMが配信装置から端末装置に放送される。端末装置は、ECMを受信する度に、PKI関連情報取得指示を含んでいるか否かを判断

する。PKI関連情報取得指示がECMに含まれている場合、端末装置は、最新のCRLを、通信を介して配信装置から受信し、保持しているCRLを最新のCRLに更新する。したがって、配信装置内でCRLが更新された場合、端末装置は、ECMの利用、すなわち、コンテンツの利用に応じて、必ず最新のCRLを取得することとなるので、コンテンツの利用と連動することなく配信されるPKI関連情報を端末で確実に取得するためのシステムが提供されることとなる。これにより、セキュリティ確保と、PKI関連情報を配信するコストの低減とが図られることとなる。

[0109] なお、第1の実施形態では、配信装置および端末装置を機能ブロックで構成することとしたが、図3に示した動作フローを実現するプログラムをCPU、通信装置、記憶装置等からなる汎用のコンピュータ装置に実行させることによって、配信装置および／または端末装置を実現するようにしてもよい。

[0110] また、配信装置および端末装置を構成する各機能ブロックは、複数の集積回路によって実現されてもよいし、一つの集積回路によって実現されてもよい。

[0111] なお、好ましくは、PKI関連情報は、SAC(Secure Authenticated Channel)と呼ばれるプロトコルによる安全な通信チャネル中で送信されるとよい。

[0112] なお、PKI関連情報を取得するには、端末装置は配信装置と相互に接続されなければならないが、その配信装置の接続先は、PKI関連情報取得指示と共に指定されているとよい。また、PKI関連情報取得指示とは別に、接続先が指定されていてもよい。また、接続先が、端末装置の出荷時などに端末装置内部のメモリ等に書き込まれることにより、予め端末装置内に指定されていてもよい。

[0113] なお、第1の実施形態では、PKI関連情報を配信装置から取得することとしたが、端末装置は、ホームネットワークの他の端末(ホームサーバを含む)から、PKI関連情報を取得してもよい。

[0114] なお、第1の実施形態では、ECMにPKI関連情報取得指示を含ませることとしたが、ユーザ毎(端末装置毎)に送信するEMM(Entitlement Management Message:個別情報)や、サーバ型放送のTypeI(ストリーム型蓄積コンテンツ)におけるECM—KcおよびKc配信用ECM、Kc配信用EMM、サーバ型放送のTypeIIコンテンツ(ファイル型蓄積コンテンツ)におけるACI(Account Control Information)な

ど、コンテンツの利用に必要となる情報にPKI関連情報取得指示を含ませてもよい。

[0115] すなわち、第1の実施形態において、配信装置は、コンテンツの利用に必要な情報と共に、PKI関連情報取得指示を送出し、端末装置は、配信装置から送出されたPKI関連情報取得指示を受信した場合、最新のPKI関連情報を取得するとよい。

[0116] (第2の実施形態)

図4は、本発明の第2の実施形態に係る情報配信システムの機能的構成を示すブロック図である。図4において、情報配信システムは、配信装置110と、端末装置210とを備える。なお、図4において、端末装置210は、一つであるとしたが、二つ以上であってもよい。この場合、各端末装置は、配信装置110からの放送を受信可能であればよい。

[0117] 配信装置110は、ECM情報蓄積部101と、ECM生成部102と、放送信号多重送信部113と、PKI関連情報取得指示付加判定部104と、PKI関連情報蓄積部105と、PKI関連情報読出部111とを含む。図4に示す配信装置110において、第1の実施形態に係る配信装置100と同様の機能を有する部分については、同一の参照符号を付し、説明を省略することとする。

[0118] PKI関連情報読出部111は、PKI関連情報蓄積部105からPKI関連情報を読み出して、放送信号多重送信部113に渡す。

[0119] 放送信号多重送信部113は、コンテンツと、ECM生成部102が生成したECMと、PKI関連情報読出部111が読み出したPKI関連情報とを多重化して放送する。PKI関連情報は、別途、エンジニアリングスロットと呼ばれる周波数帯で配信され、最終的に放送波に多重化されて送出される。

[0120] 端末装置210は、チャンネル選択部201と、放送信号受信分離部212と、ECM取得部204と、PKI関連情報取得判定要求部205と、PKI関連情報保持部206と、PKI関連情報更新部208と、PKI関連情報選択受信部211とを含む。図4に示す端末装置210において、第1の実施形態に係る端末装置200と同様の機能を有する部分については、同一の参照符号を付し、説明を省略することとする。

[0121] 放送信号受信分離部212は、チャンネル選択部201によって選択されたチャンネルのコンテンツと、ECMと、PKI関連情報とを分離する。また、放送信号受信分離部

212は、PKI関連情報選択受信部211からの指示に応じて、分離したPKI関連情報を、PKI関連情報選択受信部211に渡す。

[0122] PKI関連情報選択受信部211は、PKI関連情報取得判定要求部205からのPKI関連情報取得要求に応じて、放送信号から分離されたPKI関連情報を渡すよう放送信号受信分離部212に要求する。また、配信装置200からのPKI関連情報取得指示が無い場合でも、定常的に放送信号に多重されているPKI関連情報を放送信号受信分離部212から取得する。

[0123] 図5は、配信装置110のECM生成部102が生成するECMのデータ構造を示す図である。図5において、ECMは、ECMセクションの中に、セクションヘッダ、ECM本体、および誤り検出情報(セクションテーラ)を含む。ECM本体は、コンテンツ鍵、PKI関連情報取得指示フラグ、可変長のプライベートデータ、および改ざん検出情報からなる。PKI関連情報取得指示フラグが、PKI関連情報取得指示を示す。

[0124] 図6は、第2の実施形態に係る情報配信システムにおける配信装置110および端末装置210の動作を示すフローチャートである。以下、図6を参照しながら、第1の実施形態に係る情報配信システムにおける配信装置110および端末装置210の動作について説明する。

[0125] まず、配信装置110のPKI関連情報取得指示付加判定部104は、PKI関連情報蓄積部105に格納されているCRLが更新されているか否かを判断する(ステップS301)。ここで、CRLが更新されたか否かの判定については、第1の実施形態の図3におけるステップ101で説明した処理と同様であるので、ここでは省略する。

[0126] CRLが更新されていないと判断された場合、ECM生成部102は、PKI関連情報取得指示が付加されていないECMを生成して、ステップS303の動作に進む。

[0127] 一方、CRLが更新されていると判断された場合、ECM生成部102は、ECM情報蓄積部101に格納されているECM情報を読み出し、CRLの更新を指示するPKI関連情報取得指示を示すフラグ(PKI関連情報取得指示フラグ)をECM情報に付加して、ECMを生成し(ステップS302)、ステップS303の動作に進む。

[0128] ステップS303において、放送信号多重送信部113は、生成されたECMと、コンテンツと、PKI関連情報読出部111が読み出したPKI関連情報とを多重化して、放送

する。

[0129] 端末装置200の放送信号受信分離部212は、受信信号をチャネル選択して、ECMをECM取得部204に渡す(ステップS401)。

[0130] 次に、PKI関連情報取得判定要求部205は、ECM取得部204が取得したECMにPKI関連情報取得指示フラグが含まれているか否かを判断して、PKI関連情報取得指示がなされているか否かを判断する(ステップS402)。

[0131] PKI関連情報取得指示フラグが含まれていない場合、端末装置200は、PKI関連情報の取得に関する処理を終了する。それと並行して、端末装置210は、コンテンツ利用部(図示せず)において、コンテンツを再生する。

[0132] 一方、PKI関連情報取得指示フラグが含まれている場合、PKI関連情報取得判定要求部205は、PKI関連情報取得要求をPKI関連情報選択受信部211に渡す。これに応じて、PKI関連情報選択受信部211は、放送信号受信分離部212に放送信号におけるエンジニアリングスロットのチャネルを選択させる(ステップS403)。次に、PKI関連情報選択受信部211は、選択したチャネルから最新のCRLを取得する(ステップS404)。次に、PKI関連情報更新部208は、PKI関連情報選択受信部211が取得した最新のCRLをPKI関連情報保持部206に格納して、CRLを更新し(ステップS405)、処理を終了する。それと並行して、端末装置210は、コンテンツ利用部(図示せず)において、コンテンツを再生する。ステップS405におけるCRLの更新処理では、PKI関連情報保持部206に保持しているCRLを上書きしても良いし、CRLのバージョン番号を比較することにより、CRLの更新が不要と判断された場合には、CRLの上書きをしないようにしても良い。

[0133] このように、第2の実施形態によれば、配信装置は、常に最新のCRLをエンジニアリングスロットで配信しており、端末装置は通常、一定の間隔など、適宜エンジニアリングスロットのTSを受信し、CRLの更新を行う。加えて、配信装置は、CRLが更新された場合、PKI関連情報取得指示フラグをECMに付加して、放送する。ECMを受信した端末装置は、ECMの中にPKI関連情報取得指示フラグが含まれている場合、エンジニアリングスロットから最新のCRLを取得して、保持しているPKI関連情報を更新する。したがって、配信装置内でCRLが更新された場合、必ず、端末装置は、

最新のCRLを取得することとなるので、コンテンツの利用と連動することなく配信されるPKI関連情報を端末で確実に取得するシステムが提供されることとなる。これにより、セキュリティ確保と、PKI関連情報を配信するコストの低減とが図られることとなる。

[0134] なお、第2の実施形態では、配信装置および端末装置を機能ブロックで構成することとしたが、図6に示した動作フローを実現するプログラムをCPU、通信装置、記憶装置等からなる汎用のコンピュータ装置に実行させることによって、配信装置および／または端末装置を実現するようにしてもよい。

[0135] また、第2の実施形態では、ECMにPKI関連情報取得指示フラグを入れ、PKI関連情報取得指示フラグが含まれている場合には、端末装置は、必ずエンジニアリングスロットのチャネルを選択するようにした。しかし、ECMにCRLのバージョン、サイズ、更新日時などを入れる場合には、端末装置は、保持しているCRLのバージョン、サイズ、更新日時と、ECMに含まれるCRLのバージョン、サイズ、更新日時とを比較し、比較の結果、CRLの更新が必要であると判断した場合、エンジニアリングスロットのチャネルを選択するようにしてもよい。このように、PKI関連情報取得指示としては、フラグのように明示的な指示以外に、CRLのバージョン等の暗示的な指示も含まれる。

[0136] すなわち、第2の実施形態において、配信装置は、コンテンツの利用に必要な情報(ECM)と共に、PKI関連情報取得指示を送出し、端末装置は、配信装置から送出されたPKI関連情報取得指示を受信した場合、最新のPKI関連情報を取得するとよい。なお、PKI関連情報取得指示と共に送出するコンテンツの利用に必要な情報は、ECM以外であってもよい。

[0137] また、配信装置および端末装置を構成する各機能ブロックは、複数の集積回路によって実現されてもよいし、一つの集積回路によって実現されてもよい。

[0138] なお、第2の実施形態において、PKI関連情報はエンジニアリングスロットで放送されることとしたが、放送のプライベートセクションに含まれて放送されてもよいし、放送のデータカルーセルに含まれて放送されてもよい。どのチャンネルからPKI関連情報を取得するかは、PKI関連情報取得指示と共に指定されていてもよいし、また、PKI関連情報指示とは別に指定されていてもよい。また、取得するチャンネルが、端末装

置の出荷時などに端末装置内部のメモリ等に書き込まれることにより、予め端末装置内で指定されていてもよい。

[0139] （第3の実施形態）

図7は、本発明の第3の実施形態に係る情報配信システムの機能的構成を示すブロック図である。図7において、情報配信システムは、配信装置120と、端末装置220とを備える。なお、図7において、端末装置220は、一つであるとしたが、二つ以上であってもよい。この場合、各端末装置は、配信装置120からの放送を受信可能であり、かつ配信装置120と通信網を介して通信可能であればよい。

[0140] 配信装置120は、PKI関連情報読出部121と、放送信号多重送信部122と、PKI関連情報蓄積部105と、情報取得指示付加判定部123と、情報取得要求処理部124と、第1の通信部107と、ライセンス蓄積部125とを含む。図7に示す配信装置120において、第1の実施形態に係る配信装置100と同様の機能を有する部分については、同一の参照符号を付し、説明を省略することとする。

[0141] ライセンス蓄積部125は、コンテンツを再生するために必要なライセンス情報をユーザ毎に格納する。

[0142] 情報取得要求処理部124は、端末装置220からライセンス情報の送信要求があった場合に、ライセンス蓄積部125に格納されている当該ユーザのライセンス情報を取得する。さらに、情報取得要求処理部124は、端末装置220からライセンス情報の送信要求があった場合に、情報取得指示付加判定部123にCRLが更新されているか否かを判断させる。

[0143] 情報取得指示付加判定部123は、情報取得要求処理部124からの要求に応じて、PKI関連情報蓄積部105を参照してCRLが更新されているか否かを判断する。更新されている場合、情報取得指示付加判定部123は、最新のCRLのサイズをPKI関連情報取得指示情報として情報取得要求処理部124に渡す。ただし、CRLに記載される無効証明書のエントリが単調増加であるとする。

[0144] なお、ここでは、情報取得指示付加判定部123が、CRLが更新されているか否かを判断するようにしたが、これに限られるものではなく、その他の判断基準により情報取得指示を付加するようにしてもよい。例えば、定期的に情報取得指示を付加したり

、情報取得指示を付加する頻度(間隔)に依ったり、取得するライセンスの種類や、ユーザ毎のライセンス取得頻度などに依ることが考えられる。

[0145] 情報取得要求処理部124は、ライセンス蓄積部125から取得したライセンス情報に情報取得指示付加判定部123からの最新のCRLのサイズを付加した通信メッセージを、第1の通信部107に端末装置220宛に送信させる。通信メッセージの送信は、SACプロトコルと呼ばれる安全な通信チャネル中で行われる。

[0146] PKI関連情報読出部121は、最新のCRLをPKI関連情報蓄積部105から読み出して、放送信号多重送信部122に渡す。

[0147] 放送信号多重送信部122は、PKI関連情報読出部121からのCRLをエンジニアリングスロットに含まれるように、コンテンツと多重化して放送する。なお、ここでは、PKI関連情報(CRL)は、コンテンツと多重化されるとしたが、放送信号と多重化されるのであれば、コンテンツ以外の信号と多重化されてもよい。

[0148] 端末装置220は、放送信号受信分離部221と、PKI関連情報選択受信部222と、PKI関連情報更新部223と、PKI関連情報取得判定要求部224と、PKI関連情報保持部206と、ライセンス情報取得部225と、第2の通信部207と、ライセンス要求部226とを含む。図7に示す端末装置220において、第1の実施形態に係る端末装置200と同様の機能を有する部分については、同一の参照符号を付し、説明を省略することとする。

[0149] ライセンス要求部226は、ユーザからの要求に応じて、配信装置120に対して、第2の通信部207を介してライセンス情報の送信を要求する。なお、図7において、ユーザからのライセンス取得要求を受け取り、ライセンス要求部226に渡す機能ブロックは省略している。

[0150] ライセンス情報取得部225は、第2の通信部207で受信された通信メッセージの中に含まれるライセンス情報を取得し、通信メッセージに含まれている最新のCRLのサイズをPKI関連情報取得判定要求部224に渡す。

[0151] PKI関連情報取得判定要求部224は、受け取った最新のCRLのサイズとPKI関連情報保持部206に格納されているCRLのサイズとを比較して、格納中のCRLが古いCRLであるか否かを判断する。古いCRLである場合、PKI関連情報取得判定要求

部224は、PKI関連情報選択受信部222にPKI関連情報を取得させる。

[0152] 放送信号受信分離部221は、コンテンツのチャンネルとエンジニアリングスロットのチャンネルなどを分離する。

[0153] PKI関連情報選択受信部222は、PKI関連情報取得判定要求部224からの指示に応じて、放送信号受信分離部221で分離されたエンジニアリングスロットからPKI関連情報を取得して、PKI関連情報更新部223に渡す。

[0154] PKI関連情報更新部223は、取得したPKI関連情報保持部206に格納して、CRLを更新する。

[0155] 図8は、配信装置120から送信される通信メッセージのデータ構造を示す図である。図8において、通信メッセージには、メッセージ識別子と、最新CRLサイズと、ライセンス情報とが含まれている。メッセージ識別子とは、SAC中でのメッセージを識別するためのコードである。最新CRLサイズとは、最新のCRLのサイズを示す情報である。ライセンス情報とは、コンテンツを復号するための暗号鍵(コンテンツ鍵)や、コンテンツの利用条件などを含む情報である。ここでは、最新CRLサイズが、PKI関連情報取得指示となる。

[0156] 図9は、第3の実施形態に係る情報配信システムにおける配信装置120および端末装置220の動作を示すフローチャートである。以下、図9を参照しながら、第3の実施形態に係る情報配信システムにおける配信装置120および端末装置220の動作について説明する。

[0157] まず、端末装置220のライセンス要求部226は、ユーザのライセンス要求を受け、配信装置120に対してライセンス情報の送信を要求する(ステップS601)。

[0158] 配信装置120の情報取得要求処理部124は、第1の通信部107を介して、端末装置220からのライセンス情報の送信要求を受信する(ステップS501)。このとき、情報取得要求処理部124は、ライセンス蓄積部125に要求された該当ユーザ(あるいは、該当端末装置200)のライセンス情報が格納されていなければ、端末装置200に対してエラーを返信する。

[0159] 次に、情報取得指示付加判定部123は、PKI関連情報蓄積部105を参照して、CRLが更新されているか否かを判断する(ステップS502)。ここで、CRLが更新された

か否かの判定については、第1の実施形態の図3におけるステップ101で説明した処理と同様であるので、ここでは省略する。

[0160] CRLが更新されていないと判断された場合、情報取得要求処理部124は、ライセンス情報を含み、かつ最新CRLサイズが含まれていない通信メッセージを生成して、ステップS505の動作に進む。

[0161] 一方、CRLが更新されていると判断した場合、情報取得指示付加判定部123は、PKI関連情報蓄積部105に格納されている最新のCRLのサイズを読み出す(ステップS503)。次に、情報取得要求処理部124は、取得したサイズをライセンス蓄積部125から読み出したライセンス情報に付加して通信メッセージを生成し(ステップS504)、ステップS505の動作に進む。

[0162] ステップS505において、配信装置120は、通信メッセージを端末装置220宛に送信する。

[0163] 端末装置220のライセンス情報取得部225は、配信装置120から送信される通信メッセージを受信して、ライセンス情報および最新CRLサイズを取得し、最新CRLサイズをPKI関連情報取得判定要求部224に渡す(ステップS602)。

[0164] 次に、PKI関連情報取得判定要求部224は、PKI関連情報保持部206を参照して、保持されているCRLのサイズを取得する(ステップS603)。次に、PKI関連情報取得判定要求部224は、端末が保持するCRLのサイズの方が、最新CRLサイズよりも小さいか否かを判断する(ステップS604)。ここで、CRLのサイズが単調増加となるようにすると、CRLのサイズが小さい方が、CRLが古いことを意味することになる。

[0165] 最新CRLサイズよりも小さくない場合、保持されているCRLは古くないとして、端末装置220は、ライセンス情報取得部225によって取得されたライセンス情報を利用してコンテンツを再生し、処理を終了する。

[0166] 一方、最新CRLサイズよりも小さい場合、保持しているCRLが古いとして、PKI関連情報取得判定要求部224は、PKI関連情報選択受信部222にエンジニアリングスロットのチャネルを選択させ(ステップS605)、最新のCRLを取得させる(ステップS606)。その後、PKI関連情報更新部223は、取得した最新のCRLをPKI関連情報保持部206に格納して、CRLを更新する(ステップS607)。そして、端末装置220は、

PKI関連情報取得処理と並行して、ライセンス情報取得部225によって取得されたライセンス情報を利用してコンテンツを再生し、処理を終了する。

[0167] このように、第3の実施形態によれば、最新のPKI関連情報が配信装置から常に放送されている状況が形成される。その上で、端末装置からライセンス情報の送信要求がなされた場合、配信装置は、CRLが更新されているか否かを判断し、更新されている場合、PKI関連情報取得指示をライセンス情報に付加して、端末装置に送信する。端末装置は、配信装置によって、PKI関連情報取得指示がなされた場合、放送されているPKI関連情報を取得し、CRLを更新する。したがって、配信装置内でCRLの更新がなされた場合、必ず、端末装置は、最新のCRLを取得した上で、ライセンス情報を用いてコンテンツを利用することとなる。よって、コンテンツの利用と連動することなく配信されるPKI関連情報を端末で確実に取得するためのシステムが提供されることとなる。これにより、セキュリティ確保と、PKI関連情報を配信するコストの低減とが図られることとなる。

[0168] すなわち、第3の実施形態において、配信装置は、コンテンツの利用に必要な情報(ライセンス情報)と共に、PKI関連情報取得指示を送出し、端末装置は、配信装置から送出されたPKI関連情報取得指示を受信した場合、最新のPKI関連情報を取得するとよい。なお、PKI関連情報取得指示と共に送出するコンテンツの利用に必要な情報は、ライセンス情報以外であってもよい。

[0169] なお、第3の実施形態では、配信装置および端末装置を機能ブロックで構成することとしたが、図9に示した動作フローを実現するプログラムをCPU、通信装置、記憶装置等からなる汎用のコンピュータ装置に実行させることによって、配信装置および／または端末装置を実現するようにしてもよい。

[0170] また、配信装置および端末装置を構成する各機能ブロックは、複数の集積回路によって実現されてもよいし、一つの集積回路によって実現されてもよい。

[0171] なお、第3の実施形態において、PKI関連情報選択受信部222は、ユーザからの指示に応じて、PKI関連情報を取得して、PKI関連情報更新部223にPKI関連情報を更新させてもよい。

[0172] なお、第3の実施形態では、図8に示すようにライセンス情報にPKI関連情報取得

指示が付加されることとしたが、SACプロトコル上でやり取りされるメッセージの中に、PKI関連情報取得指示が含まれていてもよい。SACプロトコル上で送信されるメッセージの一つであるライセンスの中に、PKI関連情報取得指示が含まれていているとよい。

[0173] なお、第3の実施形態において、PKI関連情報はエンジニアリングスロットで放送されることとしたが、放送のプライベートセクションに含まれて放送されてもよいし、放送のデータカルーセルに含まれて放送されてもよい。どのチャンネルからPKI関連情報を取得するかは、PKI関連情報取得指示と共に指定されていてもよいし、また、PKI関連情報とは別に指定されていてもよい。また、取得するチャンネルが予め端末装置内で指定されていてもよい。

[0174] (他の実施形態)

第1ー第3の実施形態では、PKI関連情報取得指示として、最新CRLのバージョン番号(図2参照)、PKI関連情報取得指示フラグ(図5参照)、または最新CRLサイズ(図8参照)が用いられることとしたが、PKI関連情報の有効期限や、作成日時、証明書エントリ数のいずれかをPKI関連情報取得指示としてもよい。このような暗示的な指示もPKI関連情報取得指示に含まれる概念である。この場合も、端末装置内に格納されている古いCRLの有効期限や、作成日時、証明書エントリ数と比較することによって、端末装置は、PKI関連情報を取得すべきか否かを判断すればよい。また、これらの組み合わせによって、端末装置は、PKI関連情報を取得すべきか否かを判断してもよい。

[0175] なお、PKI関連情報取得指示と共に送出する情報は、上述した情報に限るものではなく、コンテンツの利用に必要な情報であればよい。コンテンツの利用に必要な情報と共にPKI関連情報取得指示が送出されることによって、端末装置は、コンテンツの利用と連動して、PKI関連情報取得指示をPKI関連情報を取得することができると共に、取得を強制すべきPKI関連情報を、端末装置に確実に受信させることができる。

[0176] 第1ー第3の実施形態では、端末装置は、PKI関連情報取得指示がなされていると判断した直後にPKI関連情報を取得することとしたが(図3のステップS205, 図5の

ステップS404，図9のステップS606参照)、PKI関連情報取得指示がなされていると判断した後、所定のタイミングの後に、PKI関連情報を取得するようにしてもよい。また、このとき、端末装置毎にPKI関連情報の取得タイミングを分散させるようにしても良い。

[0177] 第1ー第3の実施形態では、配信装置からのPKI関連情報取得指示があったとき、または、ユーザからの指示があったときに、端末装置は、PKI関連情報を取得することとしたが、端末装置が定期的にPKI関連情報を取得するようにしてもよい。定期的にPKI関連情報を取得するタイミングは、時間間隔や日時指定によってなされてもよいし、ライセンスの利用回数やメタデータの利用回数などによって指定されてもよい。また、このようなタイミングは、端末装置の出荷時などに端末装置内部のメモリ等に書き込まれることによって端末装置内に予め設定されていてもよいし、放送や通信で更新するようにしてもよい。

[0178] 第1ー第3の実施形態では、PKI関連情報としてCRLが用いられることとしたが、PKI関連情報として、公開鍵証明書が配信されてもよい。このとき、公開鍵証明書は、配信装置や端末装置などの他のエンティティとSACを確立するための相互認証用の公開鍵証明書であってもよいし、メタデータなどに付与されている署名検証用であってもよい。

[0179] PKI関連情報は、ECMやEMMやライセンスなどによって放送事業者毎に配信されてもよいし、エンジニアリングスロット等を利用して、全放送事業者で共通に配信されてもよい。

[0180] 端末装置は、PKI関連情報が障害などで取得できない場合、何度かリトライを行って、PKI関連情報を取得するようにしてもよい。リトライをN(≧0)回行ったが、PKI関連情報を取得できない場合、端末装置は、ユーザに対する警告メッセージ(例えば、通信接続を確認してください、チャネルAを選択してください、など)等を表示するようにしてもよい。リトライは、上記のように回数で制限してもよいし、時間で制限してもよいし、その組み合わせで制限してもよい。これらの回数制限や時間制限も放送や通信などで更新できるようにしても良いし、システムとして固定にしても良い。

[0181] また、もし、リトライを行ってもPKI関連情報を取得できない場合、端末装置は最終

的に、コンテンツの利用などに関して少なくとも一部の機能を制限(ロック)するとよい。このときも、端末装置は、ユーザに対して通知メッセージ(例えば、通信接続が確認できないため、コンテンツの利用を一時停止します。放送局Aまでご連絡をお願いします。など)等を表示するようにしてもよい。

[0182] また、第1ー第3の実施形態では、配信装置がPKI関連情報取得指示を行うか否かを判定するようにしたが、PKI関連情報取得指示を常に指示しておき、都度、端末装置がPKI関連情報の取得が必要か否かを判定するようにしても良い。

[0183] また、第1ー第3の実施形態では、配信装置が、PKI関連情報が更新されたか否かを判定し、更新されている場合に、端末装置に対してPKI関連情報取得指示を行うようにしたが、これに限られるものではなく、例えば、一定期間、定期的にPKI関連情報取得指示を行うようにしても良い。

[0184] また、PKI関連情報としてCRLと公開鍵証明書の両方を配信する場合、PKI関連情報取得指示に、CRLに対する取得指示であるのか、公開鍵証明書に対する取得指示であるのか、両方に対する取得指示であるのか等の識別情報を設けるようにしても良い。

[0185] なお、上記実施形態では、PKI関連情報を強制的に取得するためのシステムについて開示したが、本発明は、情報を強制的に取得させるためのシステムに応用が可能である。たとえば、配信装置は、PKI関連情報の代わりに、契約情報を含むライセンスやコンテンツ、メタデータ、プログラム、セキュアな時刻情報等を配信して、端末装置は、配信装置から送信される取得指示に基づいて、これらの情報を取得するようにしてもよい。

[0186] なお、本発明におけるPKI関連情報やPKI関連情報取得指示に関する情報の伝送方式は、BSデジタル放送やデジタルCATV等のいわゆる放送波による伝送方式に限られず、ADSL(Asymmetric Digital Subscriber Line)やFTTH(Fiber to the Home)、インターネット網等を利用してブロードキャストまたはマルチキャストされる伝送方式であってもよい。

[0187] なお、配信装置は、コンテンツを放送電波以外の信号を用いて、配信するようにしてもよい。たとえば、ADSLやFTTH等を用いて、コンテンツを配信するようにしても

よい。すなわち、コンテンツの配信方法は、如何なる方法であってもよい。

[0188] 以上、本発明を詳細に説明してきたが、前述の説明はあらゆる点において本発明の例示にすぎず、その範囲を限定しようとするものではない。本発明の範囲を逸脱することなく種々の改良や変形を行うことができることは言うまでもない。

産業上の利用可能性

[0189] 本発明に係る情報配信システムならびにそれに用いられる端末装置および配信装置は、コンテンツの利用と連動することなく配信されるPKI関連情報を端末装置で確実に取得することができ、コンテンツ配信の分野等において、有用である。

請求の範囲

[1] コンテンツを配信する配信装置と、前記配信装置から配信されるコンテンツを受信する端末装置とを備える情報配信システムであって、

前記配信装置は、最新のPKI関連情報の取得を前記端末装置に要求するためのPKI関連情報取得指示に関する情報を、前記コンテンツの利用に必要な情報と共に送出し、

前記端末装置は、前記配信装置から送出された前記PKI関連情報取得指示を受信した場合、最新のPKI関連情報を取得する、情報配信システム。

[2] 前記配信装置は、最新のPKI関連情報の取得を前記端末装置に要求するためのPKI関連情報取得指示に関する情報を、前記コンテンツの利用に必要な情報と共に放送するPKI関連情報取得指示放送手段を含み、

前記端末装置は、放送される前記PKI関連情報取得指示に関する情報を受信した場合、最新のPKI関連情報を取得するPKI関連情報取得手段を含む、請求項1に記載の情報配信システム。

[3] 前記配信装置は、

PKI関連情報を放送信号に多重化して放送するPKI関連情報放送手段と、

最新のPKI関連情報の取得を前記端末装置に要求するためのPKI関連情報取得指示に関する情報を、前記コンテンツの利用に必要な情報と共に前記端末装置に通信で送信するPKI関連情報取得指示送信手段とを含み、

前記端末装置は、前記配信装置からPKI関連情報取得指示に関する情報が送信されてきた場合、放送されているPKI関連情報を取得するPKI関連情報取得手段を含む、請求項1に記載の情報配信システム。

[4] 前記配信装置は、前記PKI関連情報取得手段からの要求に応じて、通信網を介して前記最新のPKI関連情報を前記端末装置に送信するPKI関連情報送信手段をさらに含み、

前記PKI関連情報取得手段は、前記配信装置から送信される前記最新のPKI関連情報を受信することを特徴とする、請求項2に記載の情報配信システム。

[5] 前記PKI関連情報送信手段は、前記最新のPKI関連情報をSAC(Secure Aut

henticated Channel)プロトコルのメッセージに含ませて送信することを特徴とする、請求項4に記載の情報配信システム。

[6] 前記PKI関連情報取得指示放送手段は、前記最新のPKI関連情報を通信で取得するための接続先を、前記PKI関連情報取得指示に関する情報と共に放送することを特徴とする、請求項4に記載の情報配信システム。

[7] 前記配信装置は、当該PKI関連情報を放送信号に多重化して放送するPKI関連情報放送手段をさらに含み、

前記PKI関連情報取得手段は、放送される前記PKI関連情報取得指示に基づいて、放送信号に多重化されて放送される最新のPKI関連情報を取得することを特徴とする、請求項2に記載の情報配信システム。

[8] 前記PKI関連情報放送手段は、前記PKI関連情報をMPEG−2 Systemsのプライベートセクションに含ませて放送することを特徴とする、請求項7に記載の情報配信システム。

[9] 前記PKI関連情報放送手段は、前記PKI関連情報をデータカルーセルに含ませて放送することを特徴とする、請求項7に記載の情報配信システム。

[10] 前記PKI関連情報取得指示放送手段は、前記最新のPKI関連情報を放送で取得するための取得先を、前記PKI関連情報取得指示に関する情報と共に放送することを特徴とする、請求項7に記載の情報配信システム。

[11] 前記PKI関連情報取得指示放送手段は、ECM(Entitlement Control Message:共通情報)またはEMM(Entitlement Management Message:個別情報)に前記PKI関連情報取得指示に関する情報を含ませて、前記ECMまたは前記EMMとコンテンツとを多重化して放送することを特徴とする、請求項2に記載の情報配信システム。

[12] 前記PKI関連情報取得指示に関する情報は、PKI関連情報取得指示を示すフラグであり、

前記PKI関連情報取得手段は、前記フラグを参照して、前記最新のPKI関連情報を取得すべきか否かを判断することを特徴とする、請求項2に記載の情報配信システム。

[13] 前記PKI関連情報取得指示に関する情報は、PKI関連情報の有効期限、作成日時、バージョン、サイズ、または証明書エントリ数のいずれか、もしくは、これらの組み合わせであり、

前記PKI関連情報取得手段は、端末装置に格納されているPKI関連情報の有効期限、作成日時、バージョン、サイズ、または証明書エントリ数のいずれか、もしくは、これらの組み合わせと、前記PKI関連情報取得指示に関する情報とを比較することによって、前記最新のPKI関連情報を取得すべきか否かを判断することを特徴とする、請求項2に記載の情報配信システム。

[14] 前記PKI関連情報取得手段は、比較の結果、前記PKI関連情報が更新されていると判断した場合、前記最新のPKI関連情報を取得することを特徴とする、請求項13に記載の情報配信システム。

[15] 前記PKI関連情報は、CRL(Certificate Revocation List:証明書失効リスト)であることを特徴とする、請求項2に記載の情報配信システム。

[16] 前記PKI関連情報は、公開鍵証明書であることを特徴とする、請求項2に記載の情報配信システム。

[17] 前記配信装置は、格納するPKI関連情報が更新されたか否かを判断するPKI関連情報更新判断手段をさらに含み、

前記PKI関連情報取得指示放送手段は、前記PKI関連情報更新判断手段によってPKI関連情報が更新されたと判断された場合、前記PKI関連情報取得指示に関する情報を、前記コンテンツの利用に必要な情報と共に放送する、請求項2に記載の情報配信システム。

[18] 前記PKI関連情報取得指示送信手段は、前記端末装置へのSACプロトコルのメッセージに前記PKI関連情報取得指示に関する情報を含ませて送信すること特徴とする、請求項3に記載の情報配信システム。

[19] 前記PKI関連情報取得指示送信手段は、SACプロトコル中で送信するライセンスに前記PKI関連情報取得指示に関する情報を含ませることを特徴とする、請求項18に記載の情報配信システム。

[20] 前記PKI関連情報放送手段は、前記PKI関連情報をMPEG−2 Systemsのプラ

イベートセクションに含ませて放送することを特徴とする、請求項3に記載の情報配信システム。

[21] 前記PKI関連情報放送手段は、前記PKI関連情報をデータカルーセルに含ませて放送することを特徴とする、請求項3に記載の情報配信システム。

[22] 前記PKI関連情報取得指示送信手段は、前記最新のPKI関連情報を放送で取得するための取得先を、前記PKI関連情報取得指示に関する情報と共に送信することを特徴とする、請求項3に記載の情報配信システム。

[23] 前記PKI関連情報取得指示に関する情報は、PKI関連情報取得指示を示すフラグであり、

前記PKI関連情報取得手段は、前記フラグを参照して、前記最新のPKI関連情報を取得すべきか否かを判断することを特徴とする、請求項3に記載の情報配信システム。

[24] 前記PKI関連情報取得指示に関する情報は、PKI関連情報の有効期限、作成日時、バージョン、サイズ、または証明書エントリ数のいずれか、もしくは、これらの組み合わせであり、

前記PKI関連情報取得手段は、端末装置に格納されているPKI関連情報の有効期限、作成日時、バージョン、サイズ、または証明書エントリ数のいずれか、もしくは、これらの組み合わせと、前記PKI関連情報取得指示に関する情報とを比較することによって、前記最新のPKI関連情報を取得すべきか否かを判断することを特徴とする、請求項3に記載の情報配信システム。

[25] 前記PKI関連情報取得手段は、比較の結果、前記PKI関連情報が更新されていると判断した場合、前記最新のPKI関連情報を取得することを特徴とする、請求項24に記載の情報配信システム。

[26] 前記PKI関連情報は、CRLであることを特徴とする、請求項3に記載の情報配信システム。

[27] 前記PKI関連情報は、公開鍵証明書であることを特徴とする、請求項3に記載の情報配信システム。

[28] 前記配信装置は、格納するPKI関連情報が更新されたか否かを判断するPKI関連

情報更新判断手段をさらに含み、

前記PKI関連情報取得指示送信手段は、前記PKI関連情報更新判断手段によってPKI関連情報が更新されたと判断された場合、前記PKI関連情報取得指示に関する情報を、前記コンテンツの利用に必要な情報と共に前記端末装置に送信する、請求項3に記載の情報配信システム。

[29] 配信装置から配信されるコンテンツを受信する端末装置であって、

前記コンテンツの利用に必要な情報と共に、前記配信装置から送出されてくる最新のPKI関連情報の取得を前記端末装置に要求するためのPKI関連情報取得指示に関する情報を受信した場合、最新のPKI関連情報を取得する、端末装置。

[30] 放送信号に多重化して放送される最新のPKI関連情報の取得を要求するためのPKI関連情報取得指示に関する情報を受信するPKI関連情報取得指示受信手段と、

前記PKI関連情報取得指示受信手段が前記PKI関連情報取得指示に関する情報をコンテンツの利用に必要な情報と共に受信した場合、前記配信装置から放送されているPKI関連情報を取得するPKI関連情報取得手段とを含む、請求項29に記載の端末装置。

[31] 前記配信装置から通信で送信されるPKI関連情報取得指示に関する情報を受信するPKI関連情報取得指示受信手段と、

前記PKI関連情報取得指示受信手段が前記PKI関連情報取得指示に関する情報をコンテンツの利用に必要な情報と共に受信した場合、前記配信装置から放送されているPKI関連情報を取得するPKI関連情報取得手段とを含む、請求項29に記載の端末装置。

[32] 放送される最新のPKI関連情報の取得を要求するためのPKI関連情報取得指示に関する情報を受信するPKI関連情報取得指示受信手段と、

前記PKI関連情報取得指示受信手段が前記PKI関連情報取得指示に関する情報を受信した場合、前記配信装置から最新のPKI関連情報を通信で取得するPKI関連情報取得手段とを含む、請求項29に記載の端末装置。

[33] コンテンツを端末装置に配信する配信装置であって、

最新のPKI関連情報の取得を前記端末装置に要求するためのPKI関連情報取得

指示に関する情報を、前記コンテンツの利用に必要な情報と共に送出する、配信装置。

[34] PKI関連情報を放送信号に多重化して放送するPKI関連情報放送手段と、

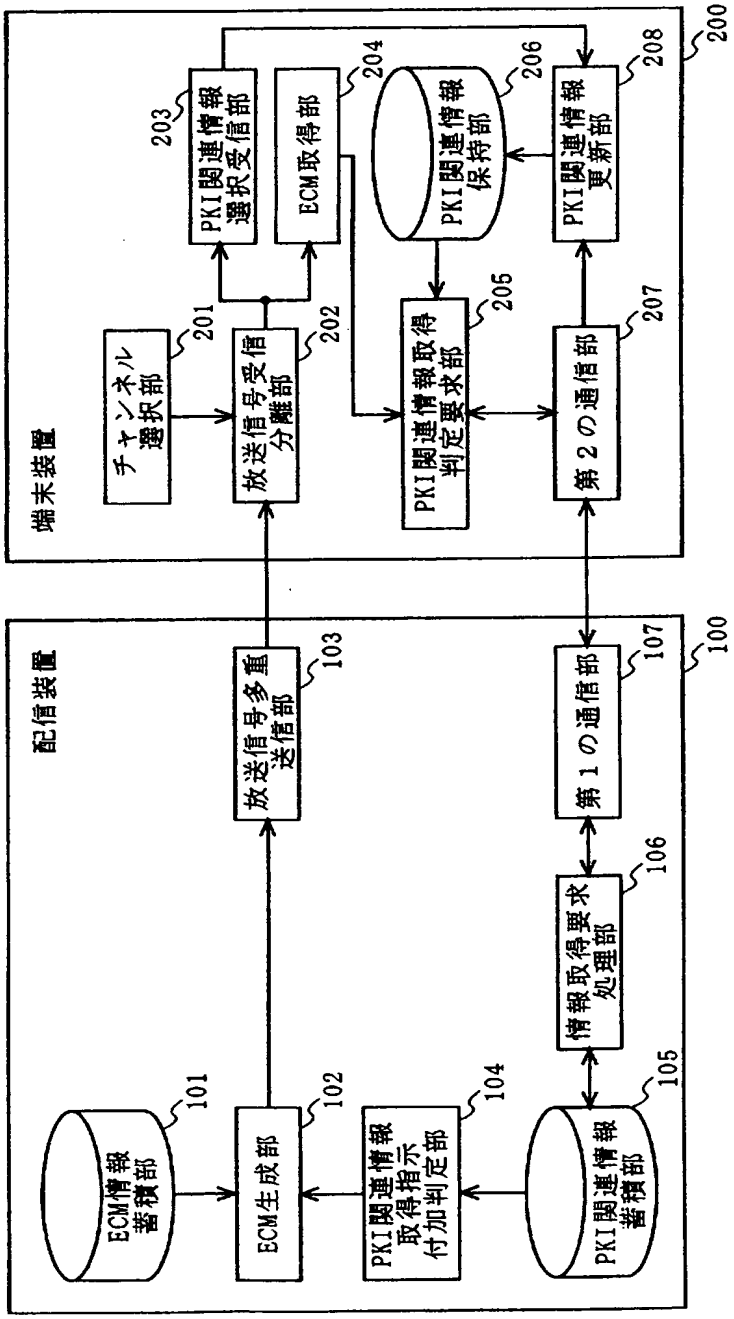
最新のPKI関連情報の取得を前記端末装置に要求するためのPKI関連情報取得指示に関する情報を、前記コンテンツの利用に必要な情報と共に放送するPKI関連情報取得指示放送手段とを含む、請求項33に記載の配信装置。

[35] PKI関連情報を放送信号に多重化して放送するPKI関連情報放送手段と、

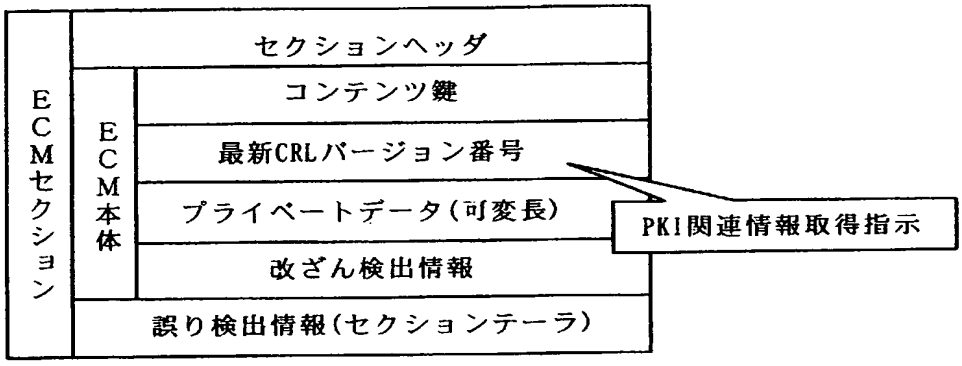
最新のPKI関連情報の取得を前記端末装置に要求するためのPKI関連情報取得指示に関する情報を、前記コンテンツの利用に必要な情報と共に前記端末装置に通信で送信するPKI関連情報取得指示送信手段とを含む、請求項33に記載の配信装置。

[36] 最新のPKI関連情報の取得を前記端末装置に要求するためのPKI関連情報取得指示に関する情報を放送するPKI関連情報取得指示放送手段を含み、前記端末装置に通信で前記最新のPKI関連情報を取得させる、請求項33に記載の配信装置。

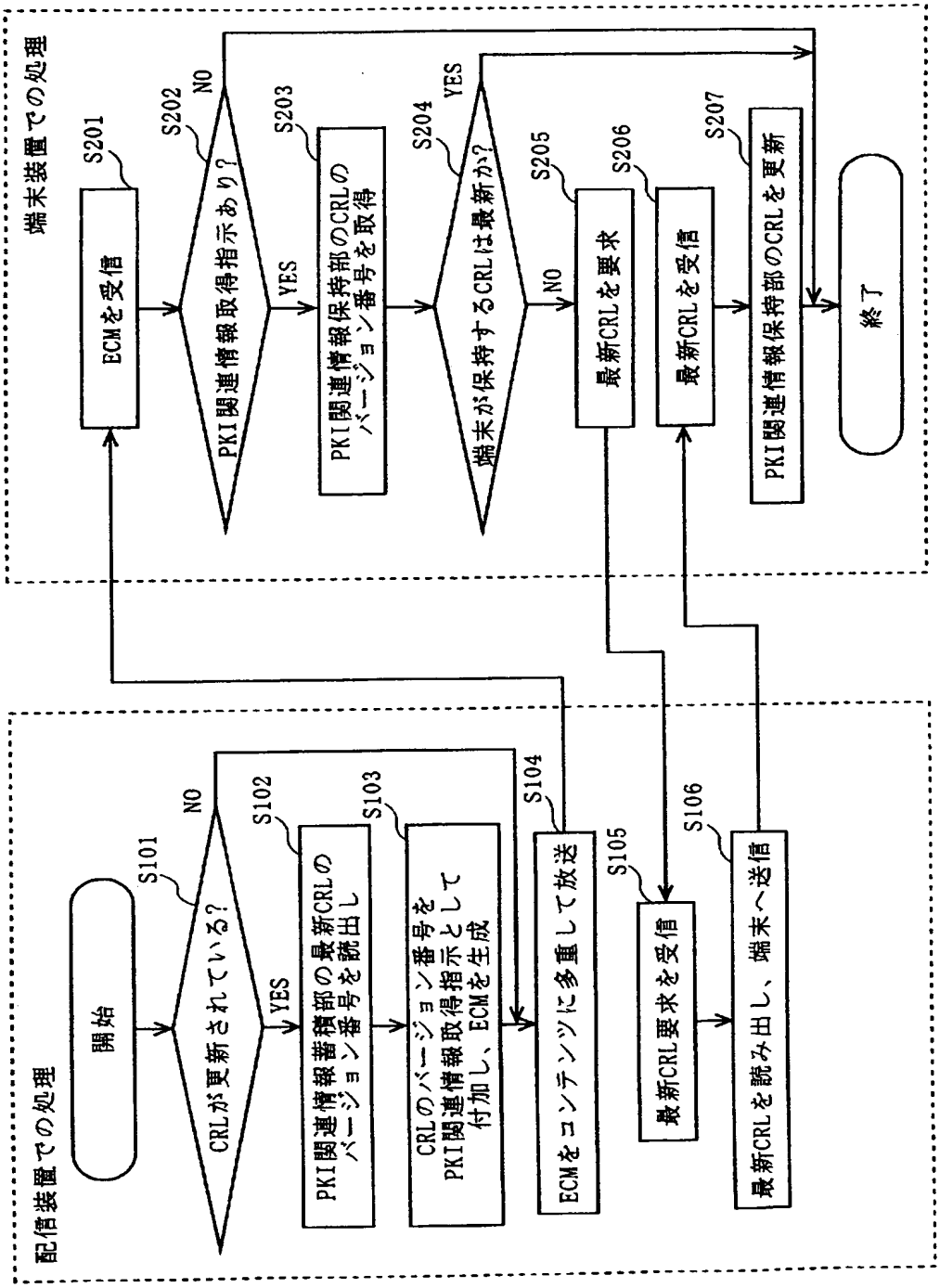
[図1]


端末装置
配信装置
チャンネル選択部
放送信号受信分離部
PKI関連情報選択受信部
ECM取得部
PKI関連情報保持部
PKI関連情報更新部
PKI関連情報取得判定要求部
第2の通信部
放送信号多重送信部
第1の通信部
情報取得要求処理部
ECM情報蓄積部
ECM生成部
PKI関連情報取得指示付加判定部
PKI関連情報蓄積部
200
201
202
203
204
205
206
207
208
100
101
102
103
104
105
106
107

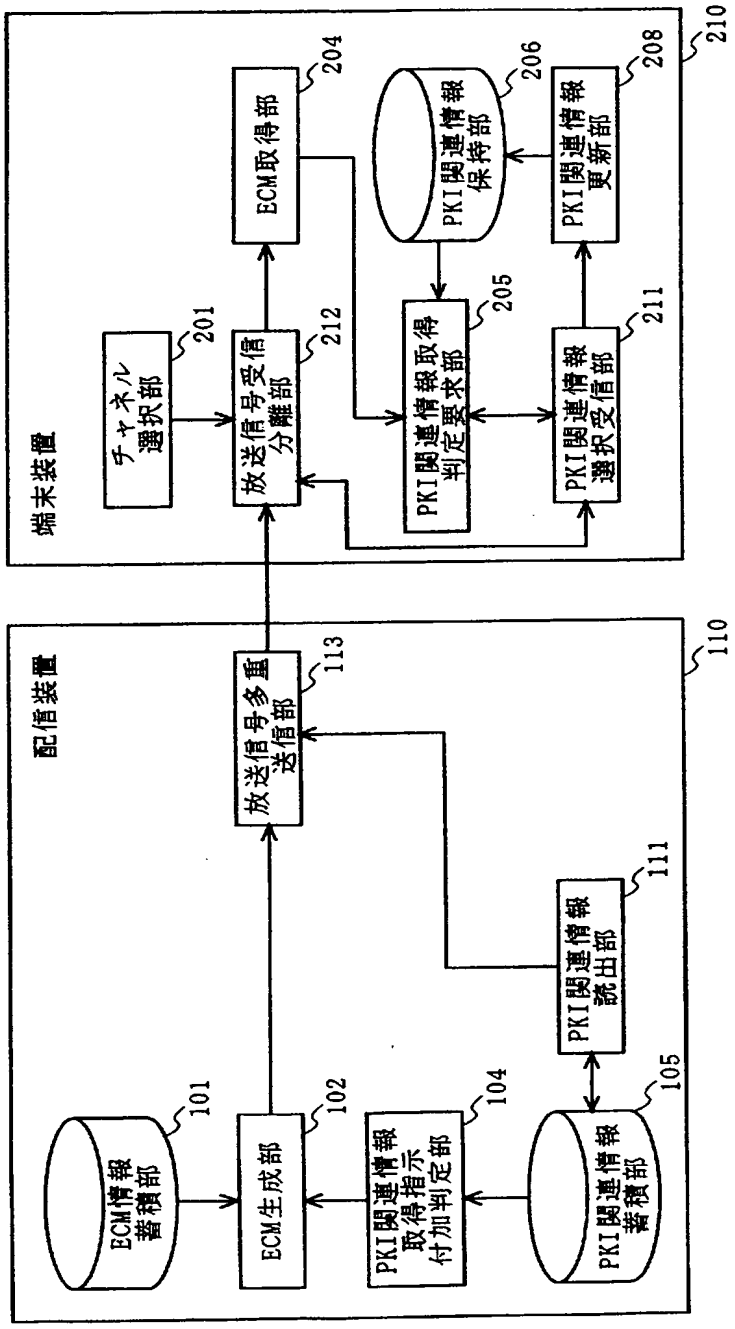
[図2]


ECMセクション
セクションヘッダ
ECM本体
コンテンツ鍵
最新CRLバージョン番号
プライベートデータ(可変長)
改ざん検出情報
誤り検出情報(セクションテーラ)
PKI関連情報取得指示

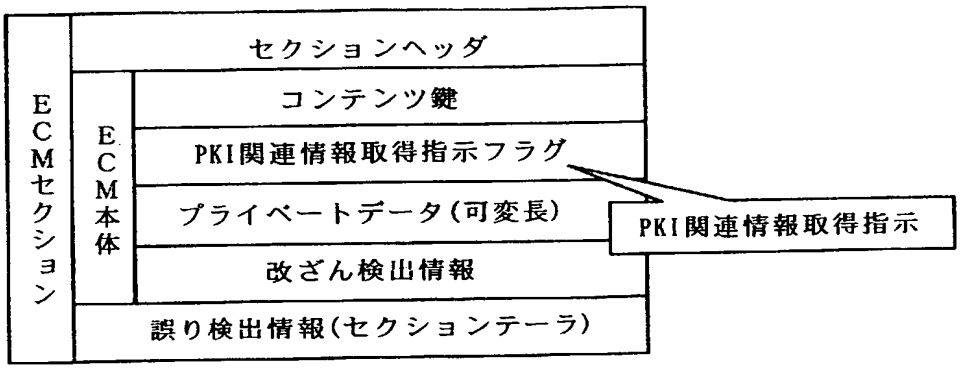
[図3]


端末装置での処理
ECMを受信
S201
PKI関連情報取得指示あり?
S202
NO
YES
PKI関連情報保持部のCRLのバージョン番号を取得
S203
端末が保持するCRLは最新か?
S204
YES
NO
最新CRLを要求
S205
最新CRLを受信
S206
PKI関連情報保持部のCRLを更新
S207
終了
配信装置での処理
開始
S101
CRLが更新されている?
NO
YES
PKI関連情報蓄積部の最新CRLのバージョン番号を読出し
S102
CRLのバージョン番号をPKI関連情報取得指示として付加し、ECMを生成
S103
ECMをコンテンツに多重して放送
S104
最新CRL要求を受信
S105
最新CRLを読み出し、端末へ送信
S106

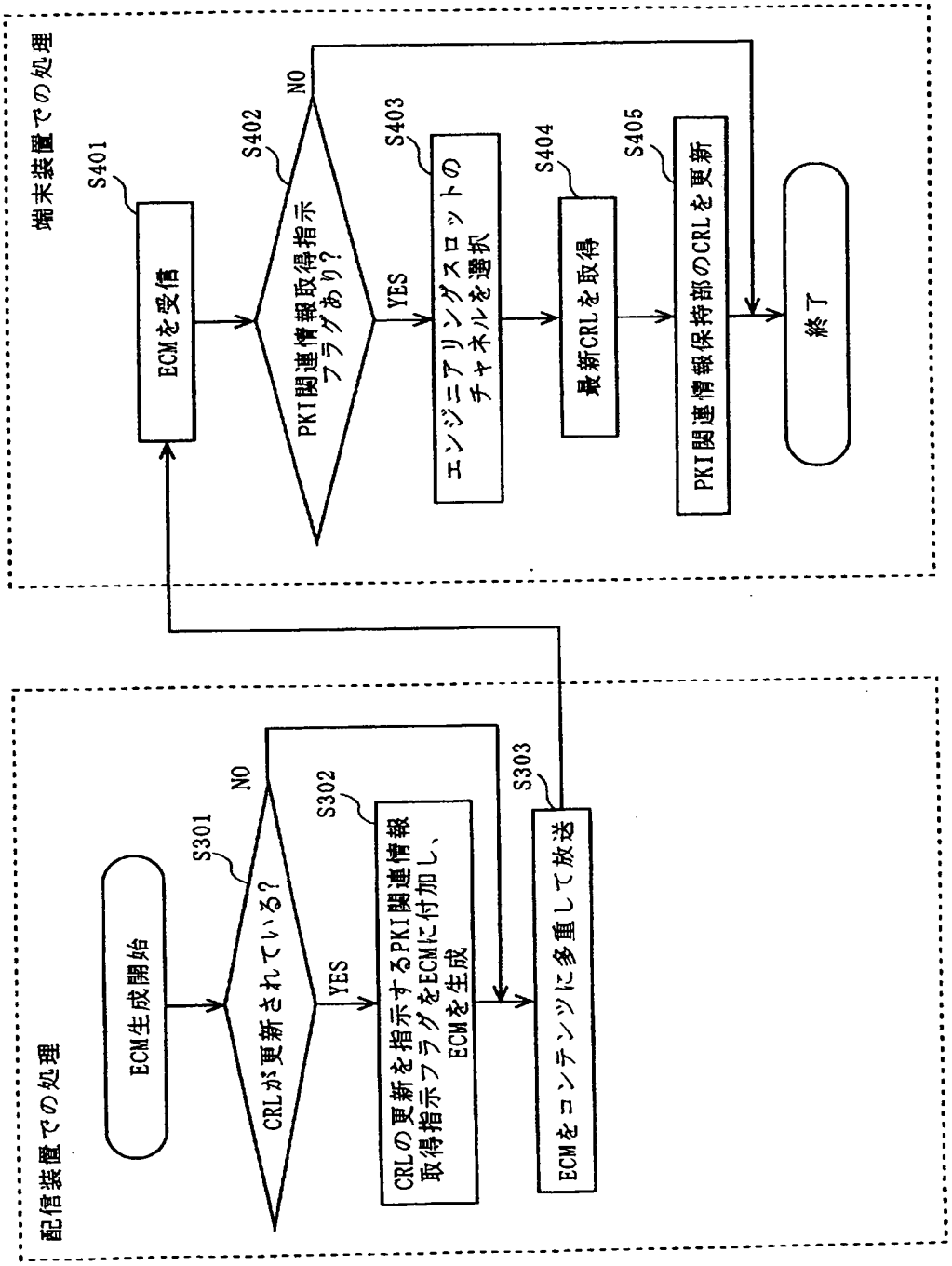
[図4]


端末装置
210
チャネル選択部
201
放送信号受信分離部
212
ECM取得部
204
PKI関連情報保持部
206
PKI関連情報更新部
208
PKI関連情報取得判定要求部
205
PKI関連情報選択受信部
211
配信装置
110
放送信号多重送信部
113
PKI関連情報読出部
111
ECM情報蓄積部
101
ECM生成部
102
PKI関連情報取得指示付加判定部
104
PKI関連情報蓄積部
105

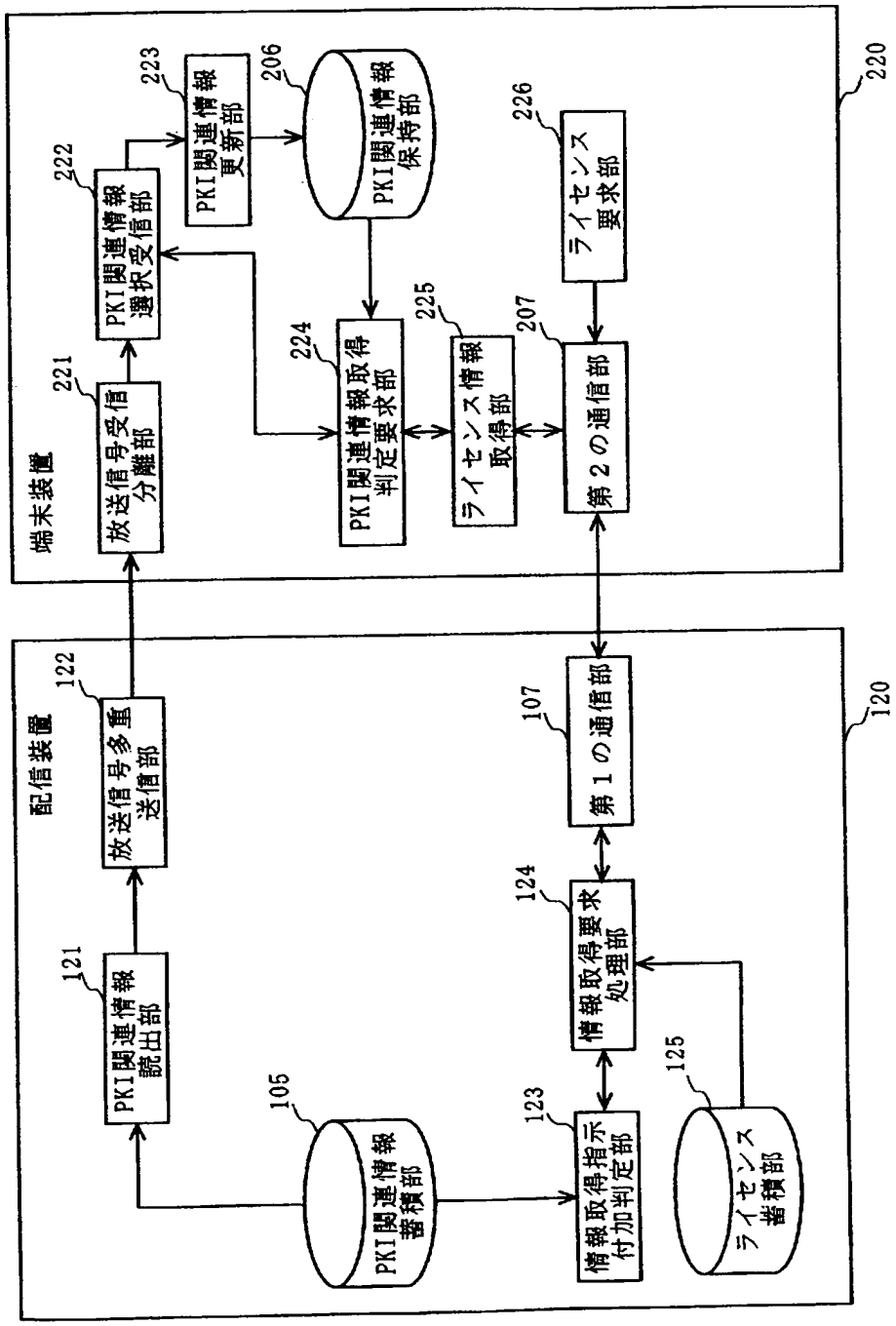
[図5]


ECMセクション
セクションヘッダ
ECM本体
コンテンツ鍵
PKI関連情報取得指示フラグ
プライベートデータ(可変長)
改ざん検出情報
誤り検出情報(セクションテーラ)
PKI関連情報取得指示

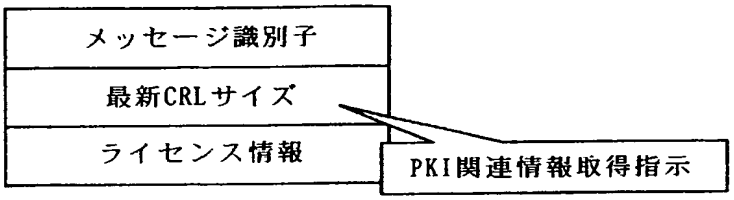
[図6]


端末装置での処理
S401
ECMを受信
S402
PKI関連情報取得指示フラグあり?
NO
YES
S403
エンジニアリングスロットのチャネルを選択
S404
最新CRLを取得
S405
PKI関連情報保持部のCRLを更新
終了
配信装置での処理
ECM生成開始
S301
CRLが更新されている?
NO
YES
S302
CRLの更新を指示するPKI関連情報取得指示フラグをECMに付加し、ECMを生成
S303
ECMをコンテンツに多重して放送

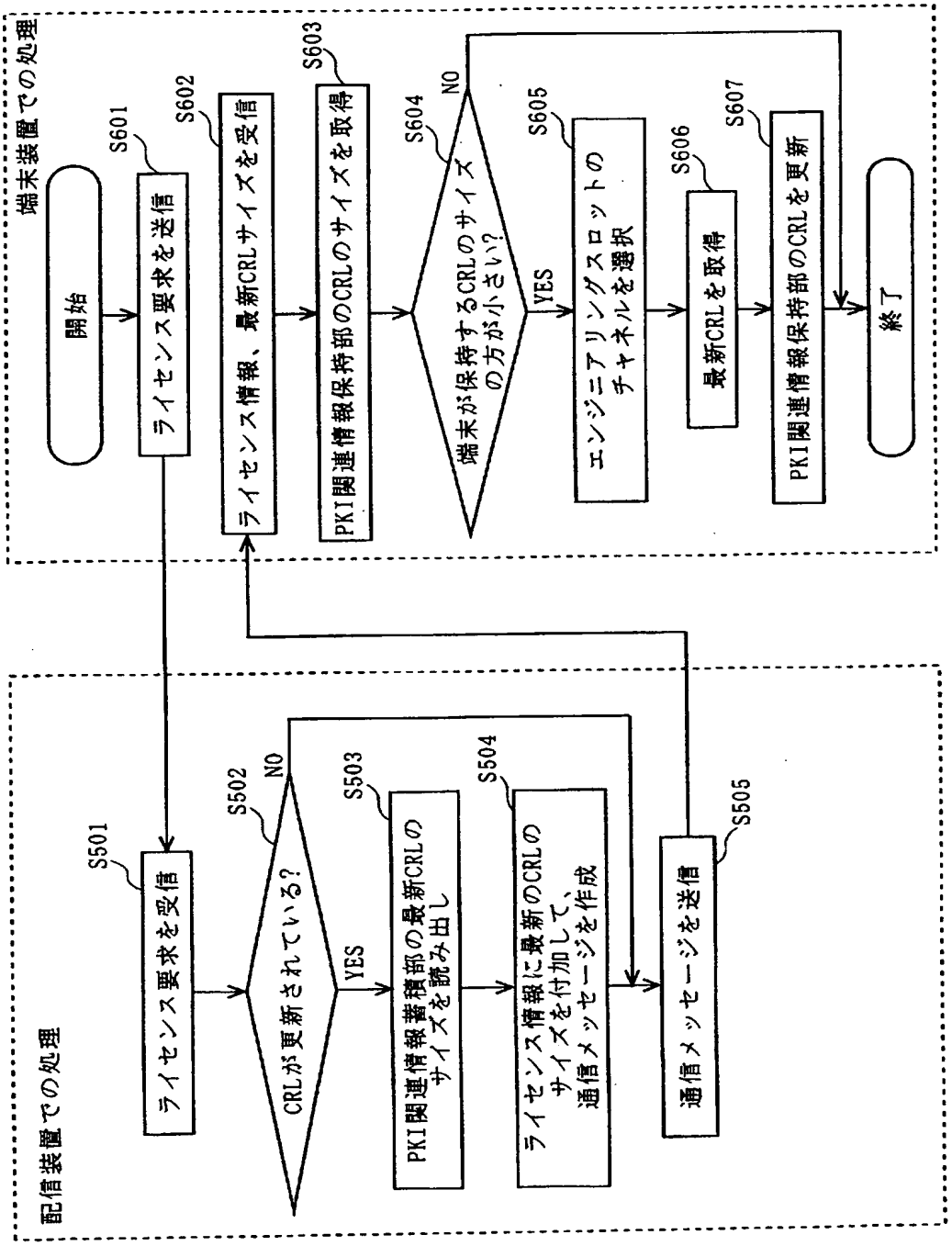
[図7]


配信装置
120
PKI関連情報読出部
121
放送信号多重送信部
122
PKI関連情報蓄積部
105
第1の通信部
107
情報取得要求処理部
124
情報取得指示付加判定部
123
ライセンス蓄積部
125
端末装置
220
放送信号受信分離部
221
PKI関連情報選択受信部
222
PKI関連情報更新部
223
PKI関連情報保持部
206
PKI関連情報取得判定要求部
224
ライセンス情報取得部
225
第2の通信部
207
ライセンス要求部
226

[図8]



[図9]


端末装置での処理
開始
S601
ライセンス要求を送信
S602
ライセンス情報、最新CRLサイズを受信
S603
PKI関連情報保持部のCRLのサイズを取得
S604
端末が保持するCRLのサイズの方が小さい?
NO
YES
S605
エンジニアリングスロットのチャネルを選択
S606
最新CRLを取得
S607
PKI関連情報保持部のCRLを更新
終了
配信装置での処理
S501
ライセンス要求を受信
S502
CRLが更新されている?
NO
YES
S503
PKI関連情報蓄積部の最新CRLのサイズを読み出し
S504
ライセンス情報に最新のCRLのサイズを付加して、通信メッセージを作成
S505
通信メッセージを送信

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/005482

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, H04L9/32, H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, H04L9/32, H04N7/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-244127 A (Canon Inc.), 29 August, 2003 (29.08.03), Par. Nos. [0098] to [0104]; Figs. 3 to 9 (Family: none)	1-36
Y	JP 2004-72717 A (Hitachi, Ltd.), 04 March, 2004 (04.03.04), Claims 2, 6 to 8; Fig. 3 & EP 1372293 A	1-36
Y	JP 2004-88279 A (Toshiba Corp.), 18 March, 2004 (18.03.04), Figs. 1 to 5 (Family: none)	5,6,8-11, 18-22

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 May, 2005 (13.05.05)	31 May, 2005 (31.05.05)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/005482

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-234728 A (Matsushita Electric Industrial Co., Ltd.), 22 August, 2003 (22.08.03), Claims 73, 74; Fig. 11 & WO 2003/30447 A	13,14,17,24, 25,28
Y	JP 2002-175084 A (Sanyo Electric Co., Ltd.), 21 June, 2002 (21.06.02), Par. No. [0121]; Fig. 10 (Family: none)	13,14,17,24, 25,28

国際調査報告

国際出願番号 PCT／JP2005／005482

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl.[7] H04L9/08 , H04L9/32 , H04N7/16

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl.[7] H04L9/08 , H04L9/32 , H04N7/16

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2005年
日本国実用新案登録公報	1996－2005年
日本国登録実用新案公報	1994－2005年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2003－244127 A（キヤノン株式会社）2003.08.29，【0098】－【0104】段落、第3－9図 （ファミリーなし）	1－36
Y	JP 2004－72717 A（株式会社日立製作所）2004.03.04，【請求項2】、【請求項6】－【請求項8】、第3図 &EP 1372293 A	1－36

☑ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 13．05．2005	国際調査報告の発送日 31.5.2005
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 5S 9469 石田 信行 電話番号 03－3581－1101 内線 3546

国際調査報告

国際出願番号 PCT／JP2005／005482

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2004－88279 A（株式会社東芝） 2004.03.18，第1－5図 （ファミリーなし）	5, 6, 8-11, 18-22
Y	JP 2003－234728 A（松下電器産業株式会社） 2003.08.22，【請求項73】、【請求項74】、第11図 &WO 2003／30447 A	13, 14, 17, 24, 25, 28
Y	JP 2002－175084 A（三洋電機株式会社） 2002.06.21，【0121】段落、第10図 （ファミリーなし）	13, 14, 17, 24, 25, 28

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005年10月6日 (06.10.2005)

PCT

(10) 国際公開番号
WO 2005/093992 A1

(51) 国際特許分類[7]: H04L 9/08, 9/32, H04N 7/16

(21) 国際出願番号: PCT/JP2005/005482

(22) 国際出願日: 2005年3月25日 (25.03.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-096222 2004年3月29日 (29.03.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真1006 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 東 吾紀男 (HIGASHI, Akio). 村上 弘規 (MURAKAMI, Hiroki). 徳田 克己 (TOKUDA, Katsumi).

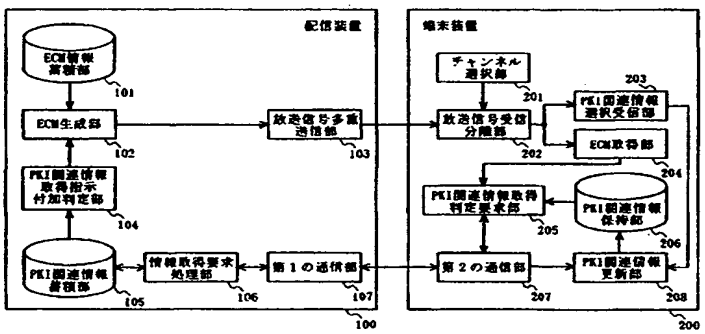
(74) 代理人: 小笠原 史朗 (OGASAWARA, Shiro); 〒5640053 大阪府吹田市江の木町3番11号第3ロンチェビル Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE,

[続葉有]

(54) Title: INFORMATION DISTRIBUTION SYSTEM

(54) 発明の名称: 情報配信システム



100...DISTRIBUTION DEVICE
101...ECM INFORMATION ACCUMULATION UNIT
102...ECM GENERATION UNIT
104...PKI-RELATED INFORMATION ACQUISITION INSTRUCTION ADDITION JUDGMENT UNIT
105...PKI-RELATED INFORMATION ACCUMULATION UNIT
106...INFORMATION ACQUISITION REQUEST PROCESSING UNIT
107...FIRST COMMUNICATION UNIT
103...BROADCAST SIGNAL MULTIPLEX TRANSMISSION UNIT
200...TERMINAL DEVICE
201...CHANNEL SELECTION UNIT
202...BROADCAST SIGNAL RECEPTION SEPARATION UNIT
203...PKI-RELATED INFORMATION SELECTION/RECEPTION UNIT
204...ECM ACQUISITION UNIT
205...PKI-RELATED INFORMATION ACQUISITION JUDGMENT REQUEST UNIT
206...PKI-RELATED INFORMATION HOLDING UNIT
207...SECOND COMMUNICATION UNIT
208...PKI-RELATED INFORMATION UPDATE UNIT

(57) Abstract: There is provided an information distribution system including a distribution device (100) for distributing a content and a terminal device (200) for receiving the content. The distribution device (100) has a PKI-related information acquisition instruction addition judgment unit (104) for judging whether the PKI-related information to be stored has been updated and a broadcast signal multiplex transmission unit (103) for multiplexing a PKI-related information acquisition instruction for requesting the terminal device to acquire the latest PKI-related information, together with the information required for the content use, on the content for broadcast when the PKI-related information acquisition instruction addition judgment unit (104) has judged that the PKI-related information has been updated. The terminal device (200) has a PKI-related information acquisition judgment request unit (205) for requesting acquisition of the latest PKI-related information when a PKI-related information acquisition instruction to be broadcast is received.

[続葉有]

WO 2005/093992 A1

ATTACHMENT A

SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: 本発明は、コンテンツを放送する配信装置（１００）と、配信装置（１００）から放送されるコンテンツを受信する端末装置（２００）とを備える情報配信システムである。配信装置（１００）は、格納するＰＫＩ関連情報が更新されたか否かを判断するＰＫＩ関連情報取得指示付加判定部（１０４）と、ＰＫＩ関連情報取得指示付加判定部（１０４）によってＰＫＩ関連情報が更新されたと判断された場合、コンテンツ利用に必要な情報と共に最新のＰＫＩ関連情報の取得を端末装置に要求するためのＰＫＩ関連情報取得指示を、コンテンツに多重化して放送する放送信号多重送信部（１０３）とを含む。端末装置（２００）は、放送されるＰＫＩ関連情報取得指示を受信した場合に最新のＰＫＩ関連情報の取得を要求するＰＫＩ関連情報取得判定要求部（２０５）を含む。